Exhibit A

The White House

Office of the Press Secretary

For Immediate Release April 20, 2010

Fact Sheet on the President's Export Control Reform Initiative

Earlier today, Secretary of Defense Robert Gates discussed the Administration's interagency review of the U.S. export control system, which calls for fundamental reform of the current system in order to enhance U.S. national security and strengthen our ability to counter threats such as the proliferation of weapons of mass destruction.

President Obama, in August of last year, initiated this comprehensive review to identify possible reforms to the system. Although the United States has one of the most robust export control systems in the world, it is rooted in the Cold War era and must be updated to address the threats we face today and the changing economic and technological landscape.

The assessment was conducted by an interagency task force created at the direction of the President and included all departments and agencies with roles in export controls. The assessment found that the current U.S. export control system does not sufficiently reduce national security risk based on the fact that its structure is overly complicated, contains too many redundancies, and tries to protect too much.

The current system is based on two different control lists administered by two different departments, three different primary licensing agencies (none of whom sees the others licenses), a multitude of enforcement agencies with overlapping and duplicative authorities, and a number of separate information technology systems (none of which are accessible to or easily compatible with the other), or agencies with no IT system at all that issues licenses. The fragmented system, combined with the extensive list of controlled items which resulted in almost 130,000 licenses last year, dilutes our ability to adequately control and protect those key items and technologies that must be protected for our national security. The goal of the reform effort is "to build high walls around a smaller yard" by focusing our enforcement efforts on our "crown jewels."

The review's overall findings have the full support of the President's senior national security team.

Key Recommendations

The Administration has determined that fundamental reform of the U.S. export control system is needed in each of its four component areas, with transformation to a:

- Single Control List,
- Single Primary Enforcement Coordination Agency,
- Single Information Technology (IT) System, and
- Single Licensing Agency.

Implementation

The Administration will engage with Congress to consult and seek its input on the proposed reforms. To deploy the new system, the Administration has prepared a comprehensive, three-phase approach and is currently moving forward to make specific reforms which can be initiated immediately and implemented without legislation. The approach will make the necessary changes to the current system to transition it to the revised, enhanced system in Phase III:

- **Phase I** makes significant and immediate improvements to the existing system and establishes the framework necessary to create the new system, including making preparations for any legislative proposals. This phase includes implementing specific reform actions already in process and initiating review of new ones.
  - **Control List** – refine, understand, and harmonize definitions to end jurisdiction confusion between the two lists; establishes new independent control criteria to be used to screen items for control into new tiered control list structure.
  - **Licensing** – implement regulatory-based improvements to streamline licensing processes and standardize policy and processes to increase efficiencies.
  - **Enforcement** – synchronize and de-conflict enforcement by creation of an Enforcement Fusion Center.
  - **IT** – determine enterprise-wide needs and begin the process to reduce confusion by creating a single U.S. Government (USG) point of entry for exporters.

- **Phase II** results in a fundamentally new U.S. export control system based on the current structure later this year. This phase completes deployment of specific Phase I reforms and initiates new actions contingent upon completion of Phase I items. Congressional notification will be required to remove munitions list controls or transfer items from the munitions list to the dual-use list, and additional funding will be required both for enhanced enforcement and the IT infrastructure.
  - **Control List** – restructure the two lists into identical tiered structures, apply criteria, remove unilateral controls as appropriate, and submit proposals multilaterally to add or remove controls.
  - **Licensing** – complete transition to mirrored control list system and fully implement licensing harmonization to allow export authorizations within each control tier to achieve a significant license requirement reduction which is compatible with national security equities.
  - **Enforcement** – expand outreach and compliance.
  - **IT** – transition toward a single electronic licensing system.
  - **Phase III** completes the transition to the new U.S. export control system. Legislation would be required for this phase:
    - **Control List** – merge the two lists into a single list, and implement systematic process to keep current.
    - **Licensing** – implement single licensing agency.
    - Enforcement – consolidate certain enforcement activities into a Primary Enforcement Coordination Agency.
    - **IT** – implement a single, enterprise-wide IT system (both licensing and enforcement).

Exhibit B

DECLARATION OF CODY WILSON

I, Cody Wilson, declare:

1. I am a citizen of the United States and a resident of Texas.

2. I co-founded and now lead Defense Distributed.

3. Defense Distributed maintains DEFCAD.com

4. Each of the ten files posted by Defense Distributed on July 27, 2018 were already in the public domain before that date, as follows:

(1) The AR-15 assembly files were available at the following sites:

Grabcad: https://grabcad.com/library/ar-15-m16-a1
CNCguns: https://www.cncguns.com/downloads.html

(2) The VZ. 58 assembly files were available at the following site:

Grabcad: https://grabcad.com/library/vz-58-rifle-1

(3) The AR-10 assembly files were available at the following site:

Grabcad: https://grabcad.com/library/ar-10-battle-rifle-7-62x51mm-1

(4) The Liberator pistol assembly files were available at the following sites:

Grabcad: https://grabcad.com/library/liberator-guns-full-1

PirateBay:
https://thepiratebay.org/torrent/8444391/DefDist_Liberator_Pistol

(5) The Beretta M9 assembly files were available at the following sites:

Grabcad: https://grabcad.com/library/beretta-92fs

(6) The 1911 assembly files were available at the following sites:

Grabcad: https://grabcad.com/library/colt-m1911-a1-2
CNCguns: https://www.cncguns.com/downloads.html

(7) The10/22 assembly files were available at the following sites:

Grabcad: https://grabcad.com/library/ruger-10-22-1
CNCguns: https://www.cncguns.com/downloads.html

(8) The Ghost Gunner 2 assembly files (not ITAR-controlled) were available at the following site:

Ghost Gunner: https://ghostgunner.net/downloads/

(9) The 308 80% lower model files were available at the following site:

CNCguns: https://www.cncguns.com/downloads.html

(10) The AR-15 80% lower model files were available at the following sites:

Grabcad: https://grabcad.com/library/mil-spec-ar-15-lower
CNCguns: https://www.cncguns.com/downloads.html

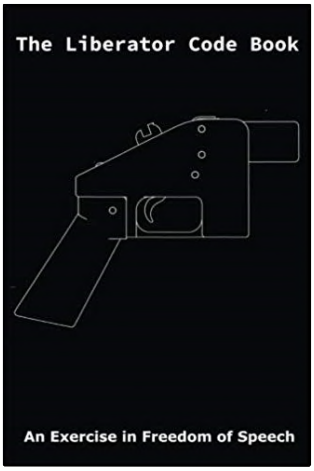
I declare under penalty of perjury that the foregoing is true and correct.

This the 15th day of August, 2018.

Cody Wilson

1000002 1

Exhibit C



The Liberator Code Book: An Exercise in the Freedom of Speech Paperback – August 1, 2018

by C J Awelow (Author)

1 customer review

#1 New Release in Computer Modelling

The purpose of this exercise is to give a physical analogy between computer code and books. Code is speech. This is a printed copy of .step files for the

Product details

Paperback: 430 pages
Publisher: CreateSpace Independent Publishing Platform (August 1, 2018)
Language: English
ISBN-10: 1724740733

ISBN-13: 978-1724740731
Product Dimensions: 6 x 1 x 9 inches
Shipping Weight: 1.6 pounds (View shipping rates and policies)
Average Customer Review: 1 customer review
Amazon Best Sellers Rank: #13,534 in Books (See Top 100 in Books)
#2 in Books > Computers & Technology > Graphics & Design > **Computer Modelling**
#2 in Books > Computers & Technology > Graphics & Design > **CAD**
#8 in Books > Arts & Photography > Architecture > **Drafting & Presentation**

Would you like to **tell us about a lower price**?
If you are a seller for this product, would you like to **suggest updates through seller support**?

Related Video Shorts (0) Upload your video

Be the first video
Your name here

Tell the Publisher!
I'd like to read this book on Kindle

Don't have a Kindle? Get your Kindle here, or download a **FREE** Kindle Reading App.

Customer reviews

1
5.0 out of 5 stars

5 star	100%
4 star	0%
3 star	0%
2 star	0%
1 star	0%

Share your thoughts with other customers

Write a customer review

See all 1 customer reviews

Search customer reviews

Search

Top customer reviews

Roadblock

I like freedom of speech!

August 11, 2018

Freedom of speech is a good thing. So is the US Consitution!

4 people found this helpful

Helpful Not Helpful Comment Report abuse

See the review

Write a customer review

Set up an Amazon Giveaway

Amazon Giveaway allows you to run promotional giveaways in order to create buzz, reward your audience, and attract new followers and customers. Learn more about Amazon Giveaway

This item: The Liberator Code Book: An Exercise in the Freedom of Speech

Set up a giveaway

Your recently viewed items and featured recommendations

See personalized recommendations

Sign in

New customer? Start here.

Back to top

Get to Know Us

Careers
Blog
About Amazon
Investor Relations
Amazon Devices

Make Money with Us

Sell on Amazon
Sell Your Services on Amazon
Sell on Amazon Business
Sell Your Apps on Amazon
Become an Affiliate
Advertise Your Products
Self-Publish with Us
› See all

Amazon Payment Products

Amazon Rewards Visa Signature Cards
Amazon.com Store Card
Amazon.com Corporate Credit Line
Shop with Points
Credit Card Marketplace
Reload Your Balance
Amazon Currency Converter

Let Us Help You

Your Account
Your Orders
Shipping Rates & Policies
Amazon Prime
Returns & Replacements
Manage Your Content and Devices
Amazon Assistant
Help

English | United States

Amazon Music — Stream millions of songs
Amazon Drive — Cloud storage from Amazon
6pm — Score deals on fashion brands
AbeBooks — Books, art & collectibles
ACX — Audiobook Publishing Made Easy
Alexa — Actionable Analytics for the Web
Amazon Business — Everything For Your Business
AmazonFresh — Groceries & More Right To Your Door
AmazonGlobal — Ship Orders Internationally
Home Services — Handpicked Pros Happiness Guarantee
Amazon Inspire — Digital Educational Resources
Amazon Rapids — Fun stories for kids on the go
Amazon Restaurants — Food delivery from local restaurants
Amazon Web Services — Scalable Cloud Computing Services
Audible — Download Audiobooks
Book Depository — Books With Free Delivery Worldwide
Box Office Mojo — Find Movie Box Office Data
ComiXology — Thousands of Digital Comics
CreateSpace — Indie Print Publishing Made Easy
DPReview — Digital Photography
East Dane — Designer Men's Fashion
Fabric — Sewing, Quilting & Knitting
Goodreads — Book reviews & recommendations
IMDb — Movies, TV & Celebrities
IMDbPro — Get Info Entertainment Professionals Need
Junglee.com — Shop Online in India
Kindle Direct Publishing — Indie Digital Publishing Made Easy
Prime Now — FREE 2-Hour Delivery on Everyday Items
Prime Photos — Unlimited Photo Storage Free With Prime
Prime Video Direct — Video Distribution Made Easy
Shopbop — Designer Fashion Brands
TenMarks.com — Math Activities for Kids & Schools
Amazon Warehouse — Great Deals on Quality Used Products
Whole Foods Market — America's Healthiest Grocery Store
Withoutabox — Submit to Film Festivals
Woot! — Deals and Shenanigans
Zappos — Shoes & Clothing
Souq.com — Shop Online in the Middle East
Subscribe with Amazon — Discover & try subscription services

Exhibit D

Details for this torrent

Type	**ThePirateBay Warning – Lawsuits & Huge fines**
Internet (Privacy)	Do NOT download any torrent before hiding your IP with a VPN. Uploaded Today 13:29, ULed by ThePirateBay

DefDist Liberator Pistol

Type:	Other > Physibles	**Uploaded:**	2013-05-06 15:22:39 GMT
Files:	20	**By:**	PrintableGunFiles
Size:	5.91 MiB (6196614 Bytes)	**Seeders:**	7
Tag(s):	DefDist Liberator Defense Distributed Printable Gun PrintableGunFiles	**Leechers:**	1
		Comments	8

Info Hash:
05A652331DD92C676B50D2FDC95E34C0CE43CB76

From the included Readme:

This is the first DD Liberator release, tested functional on 5/3/2013 and again on 5/5/2013. Design tweaks included from EXP001 and EXP002 experimental results.
Changes from EXP002:
-Barrel locking lug filet added to reduce stress concentration
-.2" hole added to handle to allow assembly without screw. AR-15 grips will fit, but need a .2" hole drilled .4x.4" from corner. Or download DD's modified AR-15 grip. This is done so you don't need a metal screw to hold the grip on.
-SN removed.
-Hammer body firing pin hole reduced to 140mils to improve firing pin concentricity on primer.
-Trigger stiffened.

How to legally assemble the DD Liberator:
-Print (ONLY) the frame sideways (the shortest dimension is the Z axis). USC18 922(p)(2)(A)*: "For the purposes of this subsection (The Undetectable Firearms Act of 1988) - the term 'firearm' does not include the frame or receiver of any such weapon;"
Thus, you can legally print ONLY the frame entirely in plastic, even without 3.7 ounces of steel.

-Once the frame is finished, epoxy a 1.19x1.19x0.99" block of steel in the 1.2x1.2x1.0" hole in front of the trigger guard. Add the bottom cover over the metal if you don't want it to show.

-Once the epoxy has tried, the steel is no longer removable, and is an integral part of the frame. Now your gun has ~6 ounces of steel and is thus considered a 'detectable' firearm. So now you can print all the other parts.

-Print all the other parts.
The barrel must be built up in the z axis.
The springs must be printed flat on their side.
The hammer body should be printed such that the firing pin hole is in the z axis.
The hammer should be printed on its side.
The trigger must be printed on its side.
The spring connecting rod bushing should be printed up in the z axis, to reduce friction.
The spring connecting rod should be printed on its side.
All pins should be printed on their side to take advantage of intralayer strength.

We'll build the trigger first. Take the trigger spring and note that there's a very small lip on one side of the ovular hole. This lip mounts flush to the trigger piece, and gives the spring enough clearance to not drag on the bottom of the inside of the frame. The spring's free ends should point away from the trigger, towards the back of the gun. Mate these two pieces, and then insert into the frame.

Next, we'll build the hammer subassembly. Insert the hammer into the hammer body with the striking cylinder facing the front of the frame. Insert the hammer pin to connect the hammer to the hammer body. Now press both coil springs onto the hammer body. When the hammer is cocked, the coil spring diameter should reduce (not expand). Once both coils are pressed on, pull one of the coil eyelets behind the hammer, and then insert the spring connecting rod into said eyelet. Rest the rod on the hammer. Slide the spring connecting rod bushing over the spring connecting rod, then pull the other spring back and insert the spring connecting rod into the eyelet. Pull the hammer back and make sure everything is working well. Pull the hammer back and drop in the nail and then insert the firing pin bushing concentric to the nail's head. This keeps the nail from falling out when the hammer is cocked. Notice that one side of the firing pin bushing is chamfered... that side faces the hammer.

Next, drop the hammer into the frame. Note that the hammer secures the trigger. Insert three frame pins to secure the hammer body.

Finally, slide the grip onto the frame and insert the grip pin. Your Liberator is now ready to go!

Before firing a barrel, we recommend heating acetone to boiling and treating the barrel for ~30 seconds to decrease the inner diameter friction, which increases barrel life from 1 round to ~10 rounds. Note that we recommend printing multiple barrels and using each only once. Swapping the barrels is simple and fast: rotate the barrel to release the locking cam. Pull up on the barrel. If the barrel cam broke, turn the Liberator upside down to remove the debris. Then drop your new barrel in and rotate it until it locks.

*http://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg3816.pdf

Comments

DakotaSmith at 2013-05-07 16:47 CET:

The Defense Distributed "Liberator" .380 single shot pistol is a fully 3D-printable firearm.

In abject violation of the Second Amendment, American lawmakers have for decades willfully, intentionally, and traitorously viol
Oaths of Office. In particular, they have destroyed the Second Amendment to the Constitution of the United States, which reads

"A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not
infringed."

The Militia is not the National Guard. As is clear from any knowledge of history, the Militia is any able-bodied citizen.

The intent of the Second Amendment is not to protect hunting nor self-defense. It is to empower the governed to overthrow the
government should it become tyrannical.

There is no question as to this intent, and any argument to the contrary betrays only a shocking ignorance on the part of the pe
making the argument.

Over the course of the 20th Century, successive generations of would-be tyrants masquerading as Congressmen, Senators, Pres
and Judges have sought to pull the teeth of the Second Amendment. Today, in abject violation of it, the United States has over
victim disarmament laws.

We can no longer defend ourselves: neither from tyrants in government, nor terrorists, nor street thugs.

This is about to change.

The Liberator is the first 3D-printable gun. You may freely download these plans and print your own. You will have available to y
capable of firing a .380 caliber bullet.

And no one -- not your next door neighbor, nor your mayor, nor your Congressman -- will know that you have it.

This is the first in what will become an avalanche of undetectable, untraceable, easy-to-manufacture weapons that will turn the
evil-doers the world over.

Share and enjoy.

ihazvpn at 2013-05-10 03:38 CET:

Thanks. Seeding forever.

ymom2 at 2013-05-10 05:14 CET:

Nice try blocking this fed lamo
#winning

kblogic at 2013-05-10 16:21 CET:

If you're having trouble loading it into Creo:

Creo doesn't support parenthesis or spaces in file names. Rename them and it will show up.

AlexLibman at 2013-05-10 22:33 CET:

Luddite govtards still think they can censor gun blueprints on the Internet...

Huge kudos to everyone for sharing and seeding!

YOU are the pillar of civilization that governments are powerless to destroy!

anotheruser1 at 2013-05-11 18:53 CET:

All government in america is pure evil, and until they are removed the threat of losing all freedom is very serious. Revolt now!

Typhoon2000 at 2013-07-24 15:34 CET:

Pro-gun people are seizing on this plastic junk as proof that guns can't ever be taken away from people by the government, whi
stupid. Even if you have a whole bunch of actual proper guns, if the feds or the cops decide to take them away, they will do so.
thing that will slow them down at all is their desire to avoid killing or hurting you in the process: your firepower is not a problem
and it really won't be a problem if all you have is a Liberator or similar.

ancap4ever at 2015-05-08 05:03 CET:

@Typhoon2000

They are based off of the pistol that were airdropped into France during WW2. French resistance members would use one to tak
German soldier and take the soldier's weapon.
They could then give the pistol to another person, and kill another German soldier.

It would be impossible for the government to disarm America, as there are just as many firearms as people.

CodeIsFreeSpeech.com

CODE IS FREE SPEECH. FREE SPEECH IS FREEDOM.

Read our statement about CodeIsFreeSpeech.com here.

FREE SPEECH FILES & CODE

- "80%" AR-15 Lower: Machining Instructions (Download) - Code (Download)
- Complete AR-15 (Download)
- Complete AR-10 (Download)
- Ruger 10-22 (Download)
- 1911 (Download)
- vz 58 (Download)
- Beretta 92FS (Download)
- Liberator (Download)- The Liberator is a physible, 3D-printable single shot handgun, the first such printable firearm design made widely available online, designed by Defense Distributed.

ABOUT THIS PROJECT

CodeIsFreeSpeech.com is a publicly-available Web site for truthful, non-misleading, non-commercial speech and information that is protected under the United States Constitution. The purpose of this project is to allow people to share knowledge and empower them to exercise their fundamental, individual rights. CodeIsFreeSpeech.com is a project of Firearms Policy Coalition, Firearms Policy Foundation, The Calguns Foundation, California Association of Federal Firearms Licensees, and a number of individuals who are passionate about the Constitution and individual liberties. We wish to thank Cody Wilson and Defense Distributed for their courage, passion, innovation, and inspiration. You can send us a message here.

SUPPORT YOUR RIGHTS AND THE PEOPLE FIGHTING FOR THEM

- Join Defense Distributed LEGIO
- Donate to Second Amendment Foundation
- Donate to Firearms Policy Coalition

- Donate to Firearms Policy Foundation
- Donate to The Calguns Foundation
- Donate to California Association of Federal Firearms Licensees

KNOW YOUR RIGHTS

United States Constitution, Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

United States Constitution, Amendment II

A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed.

United States Constitution, Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

United States Constitution, Amendment V

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

United States Constitution, Amendment XIV

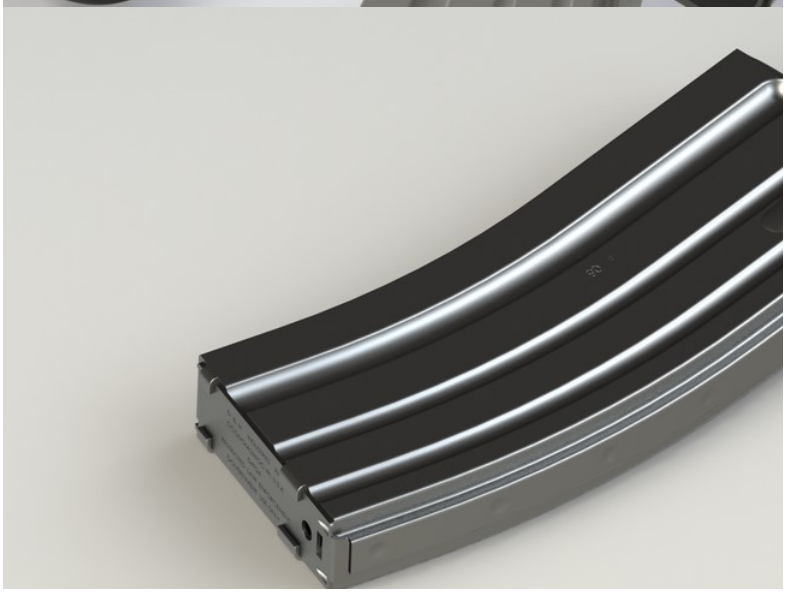
Section 1.

All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

Section 5.

The Congress shall have power to enforce, by appropriate legislation, the provisions of this article.

Join 5,040,000 engineers with over 3,020,000 free CAD files Join the Community



AR-15 M16 A1

boaz
January 13th, 2013

M16 Israeli I.D.F Version

I have tried to be as accurate as possible, but the details of some parts m

The model includes all of the parts used to make the standard weapon

Load in 3D viewer

Load in 3D viewer

Load in 3D viewer

Load in 3D viewer

Load in 3D viewer

Load in 3D viewer

Load in 3D viewer

Load in 3D viewer

Load in 3D viewer

Load in 3D viewer

Load in 3D viewer

Load in 3D viewer

Load in 3D viewer

Show more...

Download files | Like | Share

8598 Downloads236 Likes25 Comments

Details

Uploaded:January 13th, 2013
Software:Other, Rendering, SOLIDWORKS
Categories:Industrial design, Military, Tools
Tags:rifle, m16, ar15, ar, 16, assault, 15, gun, guns, arms, weapons, army, technology

236 Likes

View all

More by boaz

View all

View Files ☐

Files (21)

AR-15 M16 A1 /
M
Folder
January 20th, 2013

RT.JPG
jpg
April 6th, 2016

2.Final Color Output.png
png
April 3rd, 2013

DS.JPG
jpg
March 31st, 2013

Save Bodies2[2].sldprt
sldprt
January 20th, 2013


Fillet55.sldprt
sldprt
January 20th, 2013


M-16 Bolt 5.56.SLDPRT
sldprt
January 20th, 2013


Save Bodies3[2].sldprt
sldprt
January 20th, 2013


PKK.sldprt
sldprt
January 20th, 2013


TDI ARMS.sldprt
sldprt
January 13th, 2013


BORG.sldprt
sldprt
January 13th, 2013


DS (2).JPG
jpg
January 13th, 2013


IDIT.sldprt
sldprt
January 13th, 2013


EW.JPG
jpg
January 13th, 2013
View comments (25) ☐

Comments (25)

Please log in to add comments


Ponchai Ispersert

ผมชอบมากครับ เป็นความรู้ใหม่ของผม

28 Nov 2017 9:01 AM

Poh Swee Lay

Can anyone got the assembly to share for AR-15 M16 A1.

Thank you.

20 Sep 2017 2:18 AM


Larry

Where are all the parts?

18 Jul 2017 11:09 AM

roy yehu

where is the final part of the assembly?

9 Dec 2016 12:05 PM

yehya mahmoud

very beautiful - nice work

17 Sep 2016 9:38 AM

dart fight

Hello do you have a 3D modeling of the convertion kit 22lr ?
thank you

8 Feb 2016 8:28 AM

Load more

Downloads

Here are the files you can download for free. Currently there are three different types of files. First format is the SolidWorks E-drawings. This file format will allow anybody to open the files no matter what software you have installed. E-drawings is the most user friendly format since you don't have to have any special 3-D modeling (CAD) software to look at the files. The second format is the solid model file in *.igs format. You must have some sort of 3-D modeling (CAD) software to open this file format. If you are planning on doing the machining I have, you will need the *.igs file. But if you just want to open the file to look at it, you can download the E-drawing. And the last type of files you can download are the blueprints. I don't make blueprints of the solid models I make. So if you need a dimension while working on your project, you will have to reference the model. Later on, I hope to make available other files dealing with my projects...including sketches, setup sheets, programs, etc. Tim at dumpsterCNC made the 1911 solidmodel *.iges file. Andy at Helix60@neo.rr.com made the VZ58 *.iges file.

My files are free to download, and if you share these files they must remain free!

Download instructions

*SolidWorks E-drawings: Select the file you wish to download, click Save. To open the file, simply double click the *.exe file.*

*Solid Model *.igs File: Select the file you wish to download, click Save. Use your 3-D modeling (CAD) software to open to file after you unzip it.*

Blueprints: Select the file you wish to download, click Save. Use Adobe to open the file after you unzip it.

PayPal Donate

SolidWorks E-drawings

Select one...

Solid Model *.igs Files

Select one...

Blueprints

Select one...

The files below are complete solid models of the AR15/M16 and the 1911 firearms. I made the A2 style AR15 model, and Tom tom_eriksson@hotmail.com made the A1 style AR15 as well as the 1911 model. You can download other files Tom has made here. The files below are for visual reference only.

Complete Firearm E-drawings

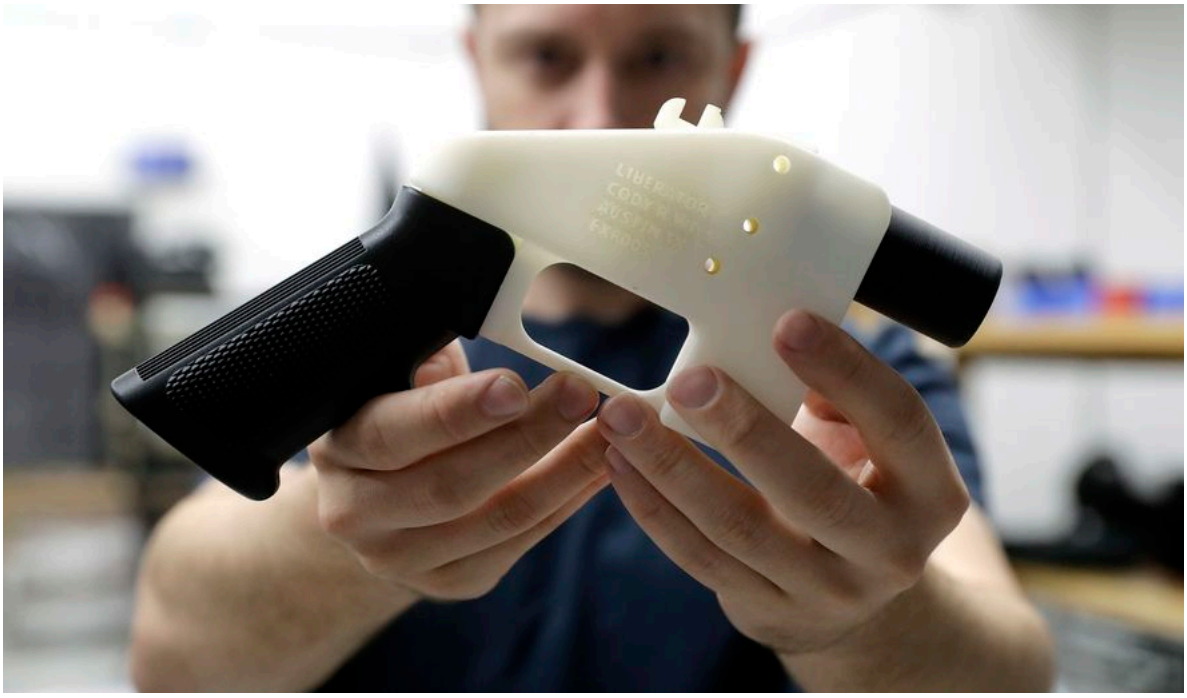
Select one...

I have spent many hours creating these solidmodel files. If you find these files useful and you want to show your support for my website, you can make a donation. All donations will be directed towards keeping this website going and also towards new projects. After every project I complete, I'll upload the files here. So if you want to show your support for this website and to keep these file FREE, you can send a donation through the PayPal link below.

PayPal Donate

Exhibit E

Judge's order backfires as activists rush to share 3D gun designs



Cody Wilson, with Defense Distributed, holds a 3D-printed gun called the Liberator at his shop, Wednesday, Aug. 1, 2018, in Austin, Texas. A federal judge in Seattle issued a temporary restraining order Tuesday to stop the release of blueprints to ... more >

By Stephen Dinan and Gabriella Muñoz - *The Washington Times - Wednesday, August 1, 2018*

A judge's attempt to halt the spread of blueprints for 3D-printed guns backfired Wednesday as the plans spread across the internet, posted and shared by people who said they were determined to strike a blow for free speech, to protect gun rights, or just to thumb their nose at the government.

Activists took to Twitter and Facebook to share links where the plans could be found on file-sharing services or sites on the dark web.

One website, CodeIsFreeSpeech.com, posted eight sets of files and reported more than 100,000 hits and nearly 1.5 terabytes of data downloaded by 6 a.m. Wednesday.

"Just in the past 48 hours, I would be shocked if hundreds of thousands of people don't possess these files," said Brandon Combs, president of the Firearms Policy Coalition, which posted the data to CodeIsFreeSpeech.

In a flurry of legal activity late Tuesday, a judge ordered the federal government to reverse itself and reimpose Obama-era export restrictions that limited the availability of the files. That order was aimed at stopping Defense Distributed, a Texas-based organization, from posting blueprints to its website, DEFCAD.com.

Cody Wilson, the site's founder, complied, but much of the rest of the internet stepped in to fill the void. "Do your human duty and share," said one Twitter user who linked to the files on a file-sharing site.

"You can't stop the flow of information," tweeted another user, duudl3, who created a mirror site to host the files Mr. Wilson disabled.

Mr. Combs and duudl3 each said his bandwidth use shot off the charts with the number of downloads.

"I've seen this stuff all over, and I suspect by the end of the next couple of days there's just going to be a saturation. They're not going to be able to do anything about it," Mr. Combs told The Washington Times.

The technology of 3D printing and plans would allow people with access to the right machinery and materials to manufacture a working, untraceable firearm in secret. The concept has existed for decades but has just recently begun to reach the mainstream, plowing new ground in the debate over gun rights and government regulations.

Some security specialists worry that the guns could circumvent metal detectors and become a tool for terrorists. Gun control activists say people banned from buying guns, such as felons and domestic abusers, also would be able to cheat the law by printing weapons at home.

Defense Distributed and like-minded groups counter that they are releasing information protected by free speech, not engaging in firearms transactions.

They also say the plans have been available for years online and there is little the government can — or should — do. Further, the possession of undetectable guns has been illegal for decades and most blueprints for 3D guns, including those of Defense Distributed, use at least some metal parts to comply with that law.

Mr. Wilson's attorneys filed court papers showing a number of other locations where blueprints for at least one home-manufactured firearm were available in 2007, a decade before Defense Distributed's planned broad release this week.

Gun control groups, which a day earlier cheered the judge's ruling as a major step for gun safety, didn't respond to a request for comment Wednesday about the fast spread of the blueprints.

Washington Attorney General Bob Ferguson, who led the lawsuit, said those still sharing the blueprints online are breaking federal export laws.

"Anyone who posts downloadable guns to the internet is violating federal law. It is the federal government's job to enforce those laws, and I urge it to enforce them aggressively as to these prohibited items," he said.

Mr. Wilson's site had planned access for blueprints for about 10 firearms. The plans govern the printing of the component parts, which would then need to be assembled.

Mr. Combs posted plans for eight firearms assemblies to his website. He said it was too early to say which one was proving most popular and that many users appeared to be downloading all of the files.

He said people are sending him new designs.

"Cody was the pioneer, and all credit goes to him and Defense Distributed," Mr. Combs said. "I just wanted to give the government another target, if that's what they want to do."

Government officials seem conflicted on what to do.

Since 2013, the State Department claimed the blueprints violated export rules, making weapons of war available to foreign actors. Mr. Wilson sued, and after a yearslong battle the Justice and State departments reversed and reached a settlement to allow Defense Distributed to move ahead with plans to post the blueprints.

The White House suggested Wednesday that Mr. Trump was blindsided by that decision.

"The Department of Justice made a deal without the president's approval on those regards," White House press secretary Sarah Huckabee Sanders said. "The president's glad this effort was delayed to give more time to review the issue, and this administration supports the decades-old legislation already on the books that prohibits the ownership of a wholly plastic gun."

Still, it's not clear what the government can do at this point.

State Department officials said their only role was to prohibit export of the blueprints outside the U.S. "The department has no role in domestic gun control policies and the broader question of this technology's potential," a spokesperson said.

Backers of 3D printing say any American has had the right to download the files, and they pointed to Wednesday's proliferation of sites as evidence that the genie is out of the bottle.

Nonetheless, lawmakers on Capitol Hill — mostly Democrats, but some Republicans — are demanding that Mr. Trump do something.

Sen. Edward J. Markey, Massachusetts Democrat, said he would try to block the confirmation of a key State Department official until the government returns to the Obama-era export policy.

The nominee, R. Clarke Cooper, has been tapped to be assistant secretary for political-military affairs, which would oversee the export rules in question.

"Until the president agrees to reverse this policy and prohibit the online publication of these dangerous blueprints, a decision that is entirely within his authority, I intend to place a hold on your nomination," Mr. Markey told Mr. Cooper.

A former chief of U.S. Capitol Police said the ability to manufacture these weapons would help bad actors circumvent security at places like the home of Congress.

"I know that a failure to permanently stop downloadable guns will increase the challenges of protecting the security of members of Congress, their staff and visitors to the Capitol," he said in an op-ed for USA Today.

Exhibit F

Export Regulation Office
600 14th ST NW Suite 300
Washington, DC 20005

VIA E-MAIL (publiccomments@bis.doc.gov AND DDTCPublicComments@state.gov)

Ms. Hillary Hess
Director, Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
Washington, DC 20230

Mr. C. Edward Peartree
Director, Office of Defense Trade Controls Policy
Directorate of Defense Trade Controls
U.S. Department of State
PM/DDTC, SA-1, 12th Floor
Washington, DC 20522

August 3, 2015

REF: RIN 0694–AG32 (BIS) AND RIN 1400-AD70 (DDTC)

RE: Comments on Proposed Revisions to Certain EAR and ITAR Definitions

Dear Ms. Hess and Mr. Peartree:

On behalf of International Business Machines Corporation ("IBM"), we are submitting these comments in response to the June 3, 2015 notices published by the Departments of Commerce and State concerning proposed revisions to definitions in the Export Administration Regulations ("EAR") and International Traffic in Arms Regulations ("ITAR") as stated in the above reference ("Proposed Rules"). These comments are timely submitted by the due date noted in the Proposed Rules.

IBM provides information technology products and services to customers in over 175 countries, and employs more than 379,000 persons across 75 countries worldwide. 2014 revenues were $92 billion, of which over 60 percent was generated outside the United States. As IBM's operations are both vast and diverse, a robust internal control program is required to ensure compliance with export regulations. Changes to the definitions within the regulations will affect the execution of the program as various areas would be impacted by the Proposed Rules, including, but not limited to the following:

- IBM's engagements involving items subject to the ITAR;
- IBM's use of cloud services for both internal and external purposes;

- Employment of foreign persons; and
- IBM's research and development functions responsible for determining the export classification of source code and technology.

IBM thanks both Departments for the opportunity to provide comments on the potential impact of the Proposed Rules. IBM supports the efforts undertaken by the Departments to improve and, wherever possible, harmonize the definitions used within the regulations as part of the Obama Administration's ongoing Export Control Reform ("ECR") initiative. It is IBM's position that many of the proposed definitions that are set forth in the Proposed Rules are an improvement on the current EAR and ITAR regulations. In particular, IBM greatly appreciates the proposed amendments to the ITAR definitions of "defense article," which would now include software and "defense services," thereby clarifying that servicing an item subject to the EAR which has been installed into a defense item would not be considered an ITAR-controlled activity.

IBM would like to offer the following recommendations for further improvements to the Proposed Rules.

RECOMMENDATIONS

1. Activities That Are Not "Exports," "Reexports," or "Transfers" (EAR § 734.18) (ITAR § 120.52)

The Proposed Rules create an exclusion from the definitions of "export," "reexport," and "transfer" for unclassified technology or software secured with end-to-end encryption using specific cryptographic modules following NIST standards and not stored in specific countries. The EAR Proposed Rule includes a provision which allows flexibility in the cryptographic methods used to meet the exclusion by including the statement "other similarly cryptographic means," whereas the ITAR Proposed Rule is rigid in its implementation.

IBM is appreciative of the exclusion and believes it will benefit industry by simplifying compliance with respect to cloud storage solutions and email transmissions; however, the use of cloud is much more pervasive and includes cloud-based software-as-a-service (SaaS) solutions and platform-as-a-service (PaaS) solutions, among others. As a result, additional exclusions are necessary to allow more freedom of action in this rapidly growing space. There is also a concern with the ITAR's proposed language, as it does not allow for industry to determine the best methods for protecting data. In addition, the referenced NIST guidance and certification requirements were not easily found.

RECOMMENDATION: IBM recommends that the proposed exclusion language in the EAR be adopted for both regulations. In addition, information on the referenced NIST guidance and certification requirements needs to be readily accessible on the Departments' web sites so users are more easily able to find the information. Lastly, IBM recommends that additional exclusions or exceptions be adopted in both regulations that would benefit cloud service providers and users

beyond the end-to-end encryption solutions for storage and email transmissions. Specifically, it would be helpful if two additional provisions were included:

a. Exclusion for the intracompany use of cloud solutions by foreign nationals directly employed by entities which have implemented a robust compliance program; and

b. Exclusion in the end-to-end encryption requirement for the decryption of data by the cloud user to perform operations within the cloud environment.

2. Activities That Are Not "Exports," "Reexports," or "Transfers" (ITAR § 120.52)

The ITAR Proposed Rule includes a provision which allows authorized foreign persons to hand carry technology and software subject to the ITAR; however, each use of this provision by the authorized foreign person must be documented.

In order for a foreign person to be authorized to obtain the technology and software in the first place, the exporter would have had to complete the export licensing process and been granted an approval. The approvals contain various provisos for use of the authorization, with which the exporter would be responsible for ensuring compliance. Adding a proviso independent from the licensing process may cause confusion for the exporter as both the license and the regulations would have to be consulted.

RECOMMENDATION: IBM recommends that any documentation requirements should be included within the licensing provisos.

3. Activities That Are Not "Deemed Reexports"

A. Requirement to Be "Certain" (EAR § 734.20(a)(2))

In the BIS Proposed Rule, a "deemed reexport" does not occur if the "technology" or "source code" is released to a foreign national, provided the entity has received it under an export authorization (i.e., license, license exception, or NLR) and, per subparagraph (a)(2), the entity must be "certain" about the foreign national's most recent citizenship.

The term "certain" indicates that the exporter must have the information verified to a level without any doubt. IBM is concerned with the amount of documentation required to achieve this standard, as well as the level of investigation needed to remove any uncertainty. Under normal hiring practices, identity and employment verification relies on standard documentation requirements (i.e., passport, permanent resident cards, and visas). This is the standard which export regulations should follow so no additional administrative burden is placed on the exporter.

RECOMMENDATION: IBM recommends the removal of the "certain" standard from the proposed language and instead to the use of a knowledge standard that is based on documentation obtained during normal hiring practices.

B. Requirement to Screen for "Substantive" Contacts (EAR § 734.20(c))

Under the proposed section, subparagraph (c) allows for an exclusion to nationals outside of Country Group A:5 as long as various conditions have been met. Under (c)(5)(ii)(B) – (D), the requirements include the need to screen the employee for "substantive" contacts with countries listed in Country Group D:5, with records maintenance at a minimum of 5 years or the duration of the employment.

This requirement is problematic in that "substantive" is an undefined term and is therefore, open to interpretation by both the exporter and the regulator. Secondly, normal business practices do not invoke a continuous screening of an individual once they have become an employee. As a result, this requirement would add administrative burden as well as a cost for conducting the additional screening throughout the span of the employee's tenure at the company. Thirdly, there is no carve out for contact with D:5 countries on behalf of the employer who may lawfully conduct business operations within the specified countries.

RECOMMENDATION: IBM recommends removal of the ongoing screening requirements from the exclusion. If this is not possible, IBM instead recommends the introduction of an exclusion for contact with D:5 countries as part of the individual's defined work scope.

4. "Peculiarly Responsible" (EAR § 772.1) (ITAR § 120.46)

The proposed definition of "peculiarly responsible" is a welcome addition to the regulations; however, it now modifies the terms which are currently included under the existing "required" definition, resulting in the introduction of the "catch and release" construct similar to that which was implemented for the term "specially designed." "Peculiarly responsible," though not defined, is a well understood concept by industry and easily explained to technical engineers and developers. The "catch and release" mechanism introduces additional complexity in that those technical personnel will now require a much broader understanding of the regulations to determine what may be controlled only for specific reasons, what may be classified as EAR99 or classified under a commodity jurisdiction, what the intent for which the item was developed, and if the item is identical to information used with items already in production. This additional complexity will complicate the classification exercise, require the inclusion of additional persons to perform this exercise, and increase the risk of classification errors by well-intentioned technical personnel who are not expert in the export regulations.

RECOMMENDATION: IBM recommends removal of the "catch and release" construct in the definition and limit the definition to "the technology or source code responsible for allowing an enumerated item to exceed the controlled performance levels, characteristics or functions."

5. "Release" (EAR §734.15; ITAR §120.50)

The proposed definition of "release" in the Proposed Rules under subparagraph (a)(1) includes "visual or other inspection" by a foreign person which reveals a controlled defense item or

"technology" or "source code" subject to the EAR. The newly defined term fails to indicate what level of access is subject to the control, which has been a historical area of confusion for industry. Specifically, does the "release" include both theoretical access and actual access, or is it limited to when an identifiable release has occurred? As an example, if a foreign person is given general access to a server which contains a database of controlled technical data, theoretical access has occurred; however, it is not until that individual visually inspects the contents of the database that controlled technical data has been provided.

RECOMMENDATION: IBM recommends both definitions be revised to indicate that "release" only occurs when EAR or ITAR controlled "technology" or "source code" has been visually inspected.

6. "Transfer" (In-Country) (EAR § 734.16) and "Retransfer" (ITAR § 120.51)

The proposed EAR definition of "transfer" and the proposed ITAR definition of "retransfer" include a change in end use as part of the defined term. This is an expansion on the current reach of the regulations. To determine a change in end use would require an exporter to continuously monitor how the exported item is being used by the third party. In a traditional sales environment, an exporter would not have visibility to how an exported item is being used unless the exporter and recipient were in a joint agreement which extends the relationship past the point of sale. This is not a typical sales model, and this level of knowledge would not be attainable during the normal course of business. Once a traditional sale is complete, the information on how the product is being used is not available.

RECOMMENDATION: IBM recommends the definitions be revised to remove a change in end use. Alternatively, the definition should be modified to indicate the obligation for the "transfer" or "retransfer" is on the ultimate consignee, not the original exporter.

7. "Defense Services" (ITAR § 120.9)

Under the proposed definition of "defense service," the Note to paragraph (a) lists various activities which are not included as a "defense service." The exclusions, specifically under number 3, include the servicing of items subject to the EAR, except as described in paragraph (a)(5) of this section. However, under (a)(5), the furnishing of assistance on a defense article or an item specially designed for a defense article to the government of a §126.1 listed country is a controlled defense service. As (a)(5) clearly defines that the items must be a defense article or an item specially designed for a defense item, the items would not be "subject to the EAR." This automatically disqualifies the activity described in exclusion number 3 to the Note to paragraph (a). As a result, the reference to the exclusion in (a)(5) is not required.

RECOMMENDATION: IBM recommends the removal of the reference to the (a)(5) exclusion in number 3 to the Note to paragraph (a).

8. "Public Domain" (ITAR § 120.11)

Under the ITAR Proposed Rule, eligibility for the release into the "public domain" of "technical data" or software hinges on a requirement to obtain a pre-approval through one of several listed U.S. government sources. In addition, in Note 1, a user is ineligible to further export, reexport or transfer information in the "public domain," if that user has "knowledge" that the information was placed in the "public domain" without obtaining the required authorizations.

The ability to place "technical data" or software in the "public domain" is protected under the First Amendment of the Constitution (i.e., freedom of speech). Placing pre-publication requirements would be a violation of an individual's fundamental rights.

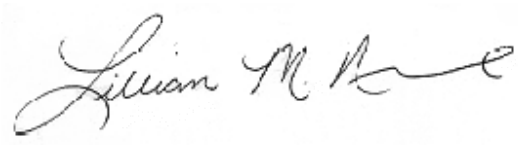
Further, depending upon the interpretation of Note 1, this Note potentially places an unnecessary burden and a risk of violation on persons which would like to further export, reexport or transfer information from a published source. The Department arguably could take the view that due diligence in this context includes verification of an existing authorization. Such an interpretation would place a burden on the user for information which has been placed in a medium where the data is considered to be freely available without restriction. In addition, without performing due diligence, any future dissemination of the data puts the user at risk of violating the regulations.

RECOMMENDATION: IBM recommends that the pre-publication requirement on information being released into the "public domain" as well as Note 1 be removed from the final rule. If Note 1 is maintained, IBM recommends that the Department specify that there is no affirmative duty on the part of users to inquire about the authorization status of information found in the "public domain."

* * *

In addition to the specific recommendations previously described, IBM believes that definitions should be consistently listed in the definitions sections of each regulation (i.e. EAR § 772 and ITAR § 120). Interspersing some definitions within the regulatory text and others within the definition sections causes confusion for industry and increases the risk of error. Placement consistency will help to alleviate that issue.

IBM feels these are the most critical changes necessary to ensure the Proposed Rules are able to be easily implemented and understood. We thank you for the opportunity to comment.



Lillian M. Norwood
Manager, Export Regulation Office
Government & Regulatory Affairs
IBM Corporation

Kathleen L. Palma
Senior Executive
International Trade Compliance
GE Corporate Legal – ITC COE

1299 Pennsylvania Ave NW
Washington D.C. 20004-2414
United States of America

T 202 637 4206
kathleen.palma@ge.com

August 3, 2015

C. Edward Peartree
Director, Office of Defense Trade Policy
Directorate of Defense Trade Controls
U.S. Department of State
Washington, D.C.

Hillary Hess
Director, Regulatory Policy Division
Office of Exporter Services
Bureau of Industry & Security
U.S. Department of Commerce
Washington, D.C.

Regulation IDs: RIN 1400-AD70 and RIN 0694-AG32

Subject: **Comments on Proposed Revisions to Definitions in the International Traffic in Arms Regulations and the Export Administration Regulations**

Dear Mr. Peartree and Ms. Hess:

General Electric Company (GE) submits the following comments in response to the Department of State, Directorate of Defense Trade Controls' (DDTC's) and the Department of Commerce, Bureau of Industry & Security's (BIS's) June 3, 2015 Proposed Rules on Revisions to Definitions in the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR), (80 Fed. Reg. 31, 525 and 80 Fed. Reg. 31, 505) (Proposed Rules). GE welcomes the opportunity to comment on the Proposed Rules.

COMMENTS PERTAINING TO THE PROPOSED DEFINITIONS OF "EXPORT"

Comments related to the revised definition of the term "Export" in ITAR §120.17 and EAR §734.13 and Activities that are Not Exports, Reexports, Releases, Retransfers, or Transfers in ITAR §120.52 and EAR §734.18

GE supports the proposed exclusions from the definitions of export for data that is secured by encryption as described in the Proposed Rules. This mechanism will provide some additional

flexibility for exporters who operate in multinational IT environments without compromising the security of the controlled data. In addition, the ability to store data outside of the U.S. will result in the ability to use lower-cost cloud options than U.S.-only cloud storage solutions. The ability to host the data closer to the customer will also improve access times globally. These benefits are substantial and the proposals represent a significant step for the U.S. Government to recognize that national borders are not the most important consideration for data security.

However, GE does have several concerns about the proposals as currently drafted. First, the requirement to use end-to-end encryption will be costly, difficult to implement and will reduce application functionality in systems that have reporting or analytic sub systems. In practice, the end-to-end encryption requirement will limit the utility of the proposal for storage of data and possibly bilateral exchange of data and will not allow the proposal to be used for other data uses. Today GE uses end-to-end encryption only in specific use cases because of the complexity involved in having the employee encrypt the data with a private key. We typically utilize environments that have strong external data security protections but do not normally require the use of end-to-end encryption. There are many other ways to protect data without the use of end-to-end encryption. If the final rules broadened this requirement to require the use of secure encryption to protect the data at all times without a specific requirement for end-to-end encryption, it would have far more utility.

Second, GE is concerned that the proposed definition of "end-to-end encryption" requires the means to access the data/keys not be given to any party other than the intended recipient. In this respect, the definition goes well beyond what is required to ensure that the data is not released to a non-U.S. person. It would be far preferable to limit the requirement not to share the data/keys with non-U.S. persons; sharing with a U.S. person IT professional inside the U.S. should not void the ability to use the provision.

Third, GE utilizes SSL Inspection Tools that decrypt data in transit, scan it for malicious code, and then re-encrypt the data with a dummy token that allows it to be passed on to the intended recipient. Without this decryption process, the malicious code inspection could not occur, potentially creating data security risks. While we have the ability to prevent data from going through one of the SSL inspection tools, our ability to prevent the data from going through another party's inspection tools is uncertain.

Fourth, with regard to the encryption standard that is authorized, GE prefers the proposed formulation in the EAR versus the ITAR in that it allows, in addition to cryptographic modules compliant with FIPS 140-2 and supplemented by procedures/controls in accordance with NIST publications, "other similarly effective cryptographic means." This standard will allow exporters to utilize a broader range of tools that will provide strong protection to controlled data. In fact, it is quite possible to be more secure than FIPS 140-2 or to be FIPS 140-2-equivalent without being FIPS certified. The NIST certification is sometimes constrained by time, and some vendors also do not wish to incur the cost. It can take six to nine months and several hundred thousand dollars to be FIPS 140-2 certified. Some software vendors, while clearly meeting the standard in practice, do not spend the time and money on such a certification. GE therefore urges the agencies to harmonize around the EAR formulation since companies that work with both ITAR and EAR data will be driven to the most restrictive standard.

The Proposed Rules restrict the countries in which controlled data can be stored, prohibiting storage of controlled data in EAR Country Group D:5 and Russia and ITAR 126.1 countries. GE requests clarification on whether data that is sufficiently encrypted to meet the requirements outlined in this Proposed Rule and that is "routed through", rather than "stored in", an EAR Country Group D:5 country, Russia, or an ITAR §126.1 country similarly would not be released from control under EAR §734.18 or ITAR §120.52.

Comments on definition of "Export of Technical Data" in ITAR §120.17(a)(6)

This section states:
§120.17 Export

> 120.17 (a)(6) - "Releasing or otherwise transferring information such as decryption keys, network access codes, passwords, or software, or providing physical access, that would allow access to other technical data in clear text or software to a foreign person regardless of whether such data has been or will be transferred . . ."

We recommend that the underlined language be revised to align the ITAR definition with the EAR definition, by incorporating concepts of "knowledge" and "actual transfer" into the definition. We suggest the following rewrite:

> 120.17(a)(6) - "Releasing or otherwise transferring decryption keys, network access codes, passwords, software or other information with knowledge that such provision will result in the transfer of other technical data in clear text (*i.e.*, in unencrypted form) or software (*i.e.*, in source code format) to a foreign person."

COMMENTS PERTAINING TO THE PROPOSED DEFINITIONS OF "TECHNICAL DATA" AND "REQUIRED"

Comments on ITAR Proposed Rule related to use of the term "technical data" in defining "required" in §120.46

GE believes that ITAR §120.46(a) may be confusing to many users because it indirectly uses the term "technical data" to define the term "technical data." In §120.10(a)(1), "technical data" is defined in terms of information required for certain defined activities. But in §120.46(a), "required" is proposed to be defined as technical data peculiarly responsible for certain controlled parameters. Since the term "required" is used in the context of identifying which information will be controlled as technical data under the ITAR, GE believes the definition would be clearer if it were modified as follows. (underscored to show changes):

> "As applied to technical data, the term required refers to only that portion of information that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions. Such required information may be shared by different products."

Conforming changes should also be made in each of Notes 1, 2 and 3 to paragraph (a).

Comments on ITAR Proposed Rule related to use of clarifying example in defining "required" in §120.46

In the EAR, the definition of "required" includes an example to help clarify that certain technology, although used in a controlled item, is not intended to be controlled because its use relates to the achievement of characteristics that are common to other commodities that are not controlled. GE believes that the ITAR should include a similar example so that information that may be useful in the development of a defense article but which has broader civil and commercial applications is not controlled. We propose that an example such as the following be included in §120.46(a):

> "... performance levels, characteristics, or functions. Such "required" information may be shared by different products. For example, assume product "X" is controlled if it is capable of operating for sustained 30 second inverted flight, and is not controlled if is merely designed to sustain an emergency flight inversion for a few seconds. If the information used in development includes technologies "A", "B", and "C" which allow inverted flight as an emergency measure but not for more than 10 seconds, then technologies "A", "B", and "C" are not "required" to develop the controlled product "X." If technologies "A", "B", "C", "D", and "E" are used together, a manufacturer can develop a product "X" that is capable of operating for sustained 30 second inverted flight. In this example, technologies "D" and "E" are "required" to make the controlled product."

Comments related to use of the term "peculiar to" in defining "required"

GE believes that using the phrase "peculiar to" in the notes to the definition of "required" (Note 1 to paragraph (a) in the ITAR, and Note 1 to the definition of "required" in the EAR) is confusing because of its similarity to the defined term "peculiarly responsible." If it is intended to mean the same thing, then GE suggests replacing the phrase "peculiar to" with "peculiarly responsible for." If the intended meaning is different than the specialized "peculiarly responsible for" term, we would alternatively recommend replacing "peculiar to" with "unique and specific to," in order to avoid confusion.

Comments related to the definition of "peculiarly responsible"

GE believes that the catch and release approach taken to define "peculiarly responsible" is one which industry will find familiar and helpful. However, we are concerned that strictly following the model used in the definition of "specially designed" results in over-regulation of information used in applications that are not military in nature. We are particularly concerned with information that has no relationship to the parameters (e.g., performance levels, characteristics, functions or other essence such as being a bomber) that cause the item to be controlled. To align this catch and release mechanism with the concept expressed in the example to the EAR definition of "required" (i.e., A, B, C, D and E), GE proposes the following 2 changes:

1) Change the "catch" paragraph of the definition as follows: "... is "peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions" if it is used in or for use in the development ... or refurbishing of the controlled parameters or portions of the item that incorporate the controlled parameters of a [defense article/item subject to the EAR] unless ..."

2) Add the following wording as release paragraph no. 2: "It is directly related to an item that is a part, component, accessory, attachment or software used in or with the defense article or item subject to the EAR that is the object of the first paragraph of this [Note/Definition];"

In addition, under the strict limitations of release paragraph no. 3, which require information to be both identical and used specifically in production items as conditions for release, a simple dimension difference between a bracket having no military functionality that is used on a military item and another bracket used on a commercial item (non-production) will be controlled even though all information and data used to design the dimensional differences themselves are commonly used in civil, non-military designs. Thus a license might be required to have this simple bracket made. GE proposes incorporating the "or equivalent" concept from the "specially designed" definition by modifying release paragraph no. 3 and adding a new Note as follows: "Is identical or equivalent in form and fit to information used in or with a commodity or software that . . ."; "Note 1 to release paragraph no. 3: With respect to information, "equivalent" means its differences relate solely to the form and fit of the commodities it is used with."

Comments related to Potential Conflict between Notes 2 and 3 to paragraph (a) of §120.46

GE believes there is a potential conflict between Notes 2 and 3 to ITAR §120.46.a. If a component subject to the EAR and under development (not in production) is incorporated or installed in a Defense Article, Note 2 indicates that the jurisdictional status of technical data directly related to development of that component is the same as the component and is not controlled under the USML. But under the catch and release mechanism of Note 3, the same technical data would be "peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions" because it is used in or for use in the development of the defense article into which the component is incorporated and there is no applicable release paragraph. As GE believes the U.S. Government's intent is to exclude technical data unless it is directly related to the controlled defense article, and not merely used in the article, GE suggests that the following words be inserted in the beginning of Note 3: "Except as described in Note 2 to paragraph (a), technical data is "peculiarly . . .."

Comments on ITAR Proposed Rule related to definition of the term "knowledge"

In Note 3 to paragraph (a) of §120.46(a), the term "knowledge" is used as an element for releasing technical data under release paragraphs 4 and 5. The use of this term for such release purposes is similar to its use in §120.41 ("specially designed") where Note 2 to Paragraphs (b)(4) and (5) defines knowledge. But that definition of "knowledge" is expressly limited to §120.41. GE recommends duplicating that definition as a new Note to Note 3 to paragraph (a) of §120.46(a). GE does not believe, however, that "knowledge" should be a separate Part 120 definition, as "knowledge" has a number of other uses in the ITAR, such as in Part 127, that have come to be understood for other specialized purposes.

Comments related to placement of the definition of "peculiarly responsible"

Comments were requested on the placement of the definition of "peculiarly responsible" in a Note to the definition of "required" versus as a stand-alone definition. GE agrees with DDTC's choice to limit its applicability to the concepts contained in §120.46. The definition of "peculiarly responsible" was

obviously given a lot of thought and written for the description of controlled technical data. The other place where the concept of "peculiarly responsible" is used is in the definition of "specially designed." The "specially designed" definition uses the term to describe properties of commodities or software to determine whether items having those properties are "specially designed." If a common definition were created, in one place it would describe an item (technical data) and in the other a non-item (properties). We are concerned that this will cause confusion for several reasons. First, there would be two distinct catch and release mechanisms operating within the "specially designed" definition, which is already complex and difficult to understand (one to determine if an item is caught under the "specially designed" part (a)(1) catch test, and the other for the "specially designed" part (b) release test). Second, use of the definition in "specially designed" would result in the anomaly of having some of the releases currently operating under part (b) of "specially designed" and adopted for the "peculiarly responsible" releases, applying to end items and materials, where those part (b) "specially designed" releases were originally intended to not apply to end items or materials.

GE also recommends that the definition of "peculiarly responsible" be removed from Part 772.1 of the EAR, and placed as Note 3 to the definition of "required."

COMMENTS PERTAINING TO THE PROPOSED DEFINITION OF "DEFENSE SERVICES"

While GE supports the clarifications and changes proposed by DDTC to the definition of "defense services" as major improvements to the earlier proposed definition, we believe that additional clarifications are necessary before a final rule is implemented.

Comments on ITAR Proposed Rule related to §120.9(a)

Use of knowledge of technical data to determine whether a defense service has been provided. GE is deeply concerned about the attempt to define defense services based on the "knowledge" of relevant technical data by the U.S. person. It is highly problematic to establish this standard based on what an engineering resource may have contained in his/her brain. This could set up truly difficult enforcement cases that do not hinge on what was actually provided to the non-U.S. entity that received the service but the knowledge of the engineer or service technician involved in providing the service. GE submits the knowledge of the individual involved should not be dispositive in determining whether a "defense service" has been provided, but rather the rules must focus on what benefits the non-U.S. entity received related to the defense article(s).

ITAR Proposed Rule Use of the term "participate." If the DDTC does not remove the knowledge requirement from the definition as suggested above, GE has additional concerns about the proposed approach. Specifically, pursuant to Note 1 to paragraph (a)(1) a person is deemed to have "knowledge of U.S.-origin technical data" directly related to a defense article if the person participated in the development of a defense article. GE believes that using participation as the threshold for determining whether a person has knowledge that rises to the level needing control as a defense service would result in the regulation of a broader set of persons than is necessary. A plain dictionary meaning of the word "participate" is "to take part in an activity." Under this definition, "participation" can include remote and indirect involvement insignificant to the actual development activities, including medical, logistical, translation, financial, legal, scheduling, and administrative services. GE proposes that the scope of deemed knowledge be narrowed to those activities that are directly related to the development activities. One way to narrow this scope would be to modify the

second sentence of Note 1 to paragraph (a)(1) to state: "... However, a person is deemed to have knowledge of U.S.-origin technical data directly related to a defense article if the person engaged in activities directly related to the development of a defense article ..."

ITAR Proposed Rule Reference to Defense Articles in the same USML paragraph. Note 1 to paragraph (a)(1) would deem a person to have "knowledge of U.S.-origin technical data" if their prior activities related to development of any defense article described in the same USML paragraph as the article that is subject of the assistance. GE believes this is also too broad because it would include involvement in the development of prior items that may have no relevance to the present assistance. For example, a person may have been involved in development of a gas turbine engine design 30 years ago (such as the J79) involving technologies that have been superseded by several generations of new engine designs. That involvement would provide little to no applicability to an advanced engine such as the F135. In addition, given the length of time, the burden on both the company and the individual to consider "participation" that is so remote in both time and relevance to the current assistance (and may require research into the actual activity for which records and memories may be scant) exceeds any benefit that U.S. Government might obtain in regulating that assistance. GE proposes narrowing the scope of the defense articles used for comparison under this provision to those that have direct relevance to the activity. One way to narrow this scope would be to further modify the second sentence of Note 1 to paragraph (a)(1) to state: "... However, a person is deemed to have knowledge of U.S.-origin technical data directly related to a defense article if the person engaged in activities directly related to the development of portions or properties of a defense article that has the same properties, and is described in the same USML paragraph as, ... the defense article that is subject of the assistance ..."

Comments on ITAR Proposed Rule related to clarification regarding the exclusions in Note to paragraph (a)

Note to paragraph (a), item no. 2 adds little guidance and may cause confusion. This item no. 2 states that performance of services by a U.S. person in the employment of a foreign person is not a defense service "except as provided in this paragraph [i.e., 120.9(a)]". Essentially, paragraph (a) provides a detailed description of what activities are defense services, and this item no. 2 states the obvious that if an activity is not described in paragraph (a) it is not a defense service. GE recommends that DDTC include examples or make a clearer statement of parameters that would be outside the scope of the description in paragraph (a). One approach could be to modify item no. 2 to state: "Performance of services by a U.S. person in the employment of a foreign person related to the production of a defense article without having the requisite knowledge described in Note 1 or Note 2 to paragraph (a)(1)."

COMMENTS PERTAINING TO THE PROPOSED DEFINITIONS OF "PUBLIC DOMAIN"

Comments on ITAR Proposed Rule related to definition of "public domain" in ITAR §120.11

GE believes that the requirement in ITAR §120.11(b) that the U.S. Government authorize all technical data or software that may be subject to the ITAR prior to release into the public domain may impose a prior restraint on the publication of privately generated unclassified information and violate the First Amendment of the U.S. Constitution. GE recommends that §120.11(b) be revised to apply only to specific types of information, such as government-funded or classified information.

Separate from the First Amendment concerns, GE questions the practicality of the proposed ITAR §120.11(b) requirement:

1. How will the Directorate of Defense Trade Controls, Office of Security Review or other relevant U.S. Government entity ensure authorization requests are processed promptly?
2. What factors will the U.S. Government rely on to determine whether authorization will be given for the release of technical data or software into the public domain?
3. How do exporters know which U.S. Government entities have the authority to issue the requisite approval for release of which technical data or software into the public domain under §§120.11(b)(3) or 120.11(b)(4)?

If DDTC proceeds with this proposed requirement notwithstanding the significant Constitutional and practical concerns, GE requests further clarity on the potential scope of §120.11(b)'s requirement. Note 1 to §120.11 states that §127.1(a)(6) prohibits the unauthorized export, reexport, retransfer or pubic release of technical data or software with knowledge that the technical data or software was made publicly available without the approval required in §120.11(b), but it does not address how technical data or information placed in the public domain without authorization prior to the effective date of this rule will be handled. It is simply unrealistic to require all technical data or software currently in the public domain without express U.S. Government authorization to receive U.S. Government authorization prior to further release, export, or rexport. GE recommends, at a minimum, the inclusion of a grandfathering clause to exempt technical data or software in the public domain prior to the effective data of the rule from §120.11(b) requirement and §127.1(a)(6).

Finally, GE requests a 6-month transition period to implement the required changes if the proposed change is finalized given the widespread effects of such a requirement.

COMMENTS PERTAINING TO THE PROPOSED DEFINITIONS OF "PERMANENT AND REGULAR EMPLOYEE"

Comments EAR Proposed Rule related to definition and use of "permanent and regular employee" in EAR §§734.20 and 750.7

GE disagrees with the proposed definition and use of the phrase "permanent and regular employee" in §§734.20 and 750.7(a) to require employment for one year or longer. In practice, the term "permanent and regular employee" generally is applied to contract or contingent workers in foreign facilities. Mandating a period of one year or longer for the relationship significantly compromises the ability of a non-U.S. defense company to take advantage of the provisions that use this phrase. Many companies do not employ contract workers for periods of a year or longer because doing so can create a risk under labor and employment law that the contract worker would take legal action to acquire the benefits and other rights of employees.

The five specific criteria enumerated under §734.20(d)(2) are adequate to ensure appropriate control of EAR data in that the worker must: (i) work at the company's facilities; (ii) work under the company's direction and control; (iii) work full time and exclusively for the company; (iv) execute nondisclosure

certifications for the company and (v) not be taking direction from the staffing company. Why is it necessary for the relationship to be "long term" if those criteria are satisfied? The company engaging the contract employee will be responsible for the conduct of the worker regardless. The company can decide the length of relationship that would be appropriate given these competing considerations.

Moreover, the timing requirement does not necessarily apply or make sense in other contexts. What if a company hires an individual for permanent employment and the employee quits after 30 days? There ultimately would be no "long term" relationship under those circumstances either, yet it is not clear in the proposed definition and use of the phrase whether the employee would fall under the "permanent and regular" definition after being hired.

GE also requests further clarification on how the proposed use of the phrase "permanent and regular employee" in §750.7 may impact existing licenses. BIS typically limits employees authorized to receive controlled data through the inclusion of conditions with the license but does not put a restriction on the amount of time an employee must be working at a facility. If the proposed changes to §750.7(a) are finalized, what happens to employees under existing licenses that do not meet the specified "permanent and regular employee" definition but were not explicitly limited in the license conditions?

GE strongly urges BIS to change the proposed language as follows:

§734.20 Activities that are not "deemed reexports."

(b) Release to A:5 nationals...

(1) * * *5 nationals...*

(2) The foreign national is a regular ~~**and permanent**~~ employee...

(c) Release to other than A:5 nationals... *R*

(1) * * *elease to other than A:5 nationals.*

(2) The foreign national is a regular ~~**and permanent**~~ employee...

(d) Definitions.*Definitions.*

(1) * * *

(2) "~~***Permanent and***~~ is an individual who:

(a) Is ~~**permanently (i.e., for not less than a year) and**~~ directly employed by an entity, or

(b) Is a contract employee who:

(i) Is in a ~~**long-term**~~ contractual relationship with the company...

§750.7(a) ... A BIS license authorizing the release of technology to an entity also authorizes the release of the same technology to the entity's foreign nationals who are ~~**permanent and**~~ regular employees (and who are not proscribed persons under U.S. law)...

COMMENTS PERTAINING TO THE PROPOSED DEFINITIONS OF "ACTIVITIES THAT ARE NOT DEEMED REEXPORTS"

Comments related to definition of "Activities that are not "deemed reexports" in EAR §734.20(c)

GE believes the requirement in §734.20(c)(5)(ii)(B) to screen for contacts in Country Group D:5 is too broad. Country Group D:5 includes countries such as China and Vietnam where, like many multinational companies, GE has major manufacturing operations and installation bases. As a result, many employees are likely to have "substantive contact" (as defined in §734.20(d)(1)) with these countries (e.g., "recent or continuing contact with agents, brokers, and nationals of such countries," "maintenance of business relationships with persons from such countries") as a normal course of business (not including technology or source code transfers). Implementation of the proposed requirement in §734.20(c)(5)(ii)(B) therefore would consume tremendous amounts of resources without yielding substantive screening results mitigating the targeted risks of diversion.

GE suggests that the requirement in §734.20(c)(5)(ii)(B) to screen for contacts in Country Group D:5 be revised to more specifically address the potential risk of diversion – e.g., change the requirement to screen for contacts in to Country Group E:1, or change the proposed language to:

§734.20 Activities that are not "deemed reexports."

(d) Definitions. (1) "Substantive contacts" includes ~~**regular travel to countries in Country Group D:5; recent or continuing contact with agents, brokers, and nationals of such countries;**~~ continued demonstrated allegiance to such countries; ~~**maintenance of business relationships with persons from such countries;**~~ maintenance of a residence in such countries; receiving salary or other continuing monetary compensation from such countries; or acts otherwise indicating a risk of diversion.

In addition, GE finds the requirement in §734.20(c)(5)(ii)(D) to maintain records for the longer of five years or the duration of individual's employment with the entity to be overly prescriptive and burdensome. GE suggests that BIS change the proposed language to:

§734.20 Activities that are not "deemed reexports."

(c) Release to other than A:5 nationals.

(5) * * *

(ii) * * *

(D) Maintains records of such screenings for ~~**the longer of five years or the duration of the individual's employment with the entity;**~~ five years after the release of "technology" or "source code" takes place.

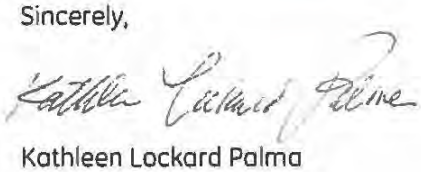
It is also worth noting that the requirements of §734.20(c)(5)(ii)(B) and 734.20(c)(5)(ii)(D) seem more restrictive than the riders and conditions with licenses that would cover the same foreign national employees from Country Group D:5. If the foreign entity can demonstrate effective compliance to §§734.20(c)(3) and 734.20(c)(4), then §§734.20(c)(5)(ii)(B) and 734.20(c)(5)(ii)(D) have very little value

considering the extra burden beyond a typical license. Given the personal data privacy laws in Europe and Canada, compliance with §§734.20(c)(5)(ii)(B) and 734.20(c)(5)(ii)(D) is even more difficult.

* * * * *

We appreciate the opportunity to provide comments on the Proposed Rules. If you have any questions or require additional information concerning this submission, please contact the undersigned at (202) 637-4206 or by email at: kathleen.palma@ge.com or George Pultz at (781) 594-3406 or by email at: george.pultz@ge.com.

Sincerely,



Kathleen Lockard Palma
International Trade Compliance

July 15, 2015

To: DDTCPublicComments@state.gov
publiccomments@bis.doc.gov

From: Bill Root, waroot23@gmail.com; tel. 517 333 8707

Subject: ITAR Amendment - Revisions to Definitions: Data Transmission and Storage
EAR Revisions to Definitions - RIN 0694-AG32

The June 3, 2015 proposed rules from the State and Commerce Departments are intended to harmonize and clarify ITAR and EAR definitions while improving national security. These comments describe many respects in which they go in the opposite direction. The six most important ones are those numbered 1 to 6 below. Those numbered 7 to 10, while less important, are still significant. At the end is an analysis of what could happen if no changes are made.

1. Prior Restraint of Public Domain Exclusion from Export Controls

The ITAR proposed requirement for USG authorization to put information into the "public domain" in 120.11(b) is a reversal of actions 30 years ago to comply with the free speech first amendment to the Constitution. EAR proposals would change "are already published or will be published" to "are published" in what is "not subject to the EAR" in 734.3(b)(3)(i) and delete "The EAR do not cover technology ... that is made public by the transaction in question" now in 734 Supplement 1. So, ITAR would explicitly challenge the Constitution and EAR would remove language which now complies with the Constitution. Remedies: Delete 120.11(b); do not revise 734.3(b)(3)(I); and do not delete 734 Supplement 1.

2. Deletion of Clarifications

The many clarifying questions and answers concerning publicly available information in EAR 734 Supplement 1 would be deleted. Remedies: Do not delete 734 Supplement 1 (a few revisions to update that Supplement are included in #10 below).

3. Over-riding "Required"

ITAR 120.46 would add the EAR and Wassenaar definition of "required" as

> "only that portion of technical data that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions."

However, per proposed Note 3, those words would ambiguously be met if technical data are for development, production, or use of a defense article unless subject to three releases now in the definition of "specially designed." EAR would add to 772.1 a definition of "peculiarly responsible" having the same effect as ITAR Note 3. "Peculiarly responsible" wording now appears not only in the definition of "required" but also in the definition of "specially designed." So, the June 3 proposals largely over-ride the substance of the "required" definition in ITAR and in the hundreds of existing uses of "required" and "specially designed" in the EAR. Remedy: Limit 120.46 Note 3 and 772.1 definition of "peculiarly responsible" to License Exceptions (for details see #10 below).

4. Violations of NSDD 189

A 1985 National Security Decision Directive (NSDD) 189 specifies:

> "where the national security requires control, the mechanism for control of information generated during federally-funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification. ... No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification ..."

The June 3 120.49, 734.8, and 734.11 proposals expand existing pre-publication review restrictions on federally-funded fundamental research other than classification. Remedy: Delete all restrictions on federally-funded fundamental research in 120.49, 734.8, and 734.11 (for details see #10 below).

5. Inadequate Control of Munitions Production

Instead of expanding unconstitutional and unenforceable controls on what is publicly available and increasing ambiguity on what technology is controlled, the United States should comply with the vastly more important multilateral controls on munitions production (WA ML 22.b.1) and missile production (MTCR 1.B.1). Several decades ago, a UK firm, Matrix Churchill, after consulting with the UK government, exported to Iraq, without a license, equipment not requiring a license but used to produce munitions. Parliamentarians severely criticized the UK government, which survived a motion of no confidence by just one vote. The UK had failed to include on its control list the following COCOM Munitions List item 22.b.1, which remains on the Wassenaar Munitions List to this day:

> Design of, assembly of components into, and operation, maintenance, and repair of complete production installations for Munition List items even if the components of such production installations are not specified.

ITAR 120.9 defense services cover "furnishing assistance to foreign persons in the production of defense articles." This is relevant. But, in 1980, DOD concluded that such general wording was insufficient. So, I led a negotiation which added ML 22.b.1. The Matrix Churchill case proved that DOD was right. Even so, in the intervening 35 years, neither State nor Commerce has seen fit to incorporate into a U.S. export control list WML 22.b.1, b.2, or b.5. WML 22.b.2 reads:

> Technology required for development or production of small arms even if used to produce reproductions of antique small arms.

WML 22.b.5 reads:

> Technology required exclusively for incorporation of biocatalysts specified in ML7.i.1 into military carrier substances or military materials.

In 1987, the Missile Technology Control Regime was established. Its main objective was to control production of missiles. Once again, ITAR defense services language was relevant. But U.S. negotiators wanted something more specific, called "production facilities," defined as:

> Production equipment and specially designed software therefor integrated into installations for development or for one or more phases of production.

Item 1.B.1, "production facilities" for missiles, has been on the MTCR list for almost three decades. But it still has not made it onto a U.S. export control list.

Remedies: add new ECCN 9B110 "Production facilities" for "development" or "production" of "missiles"; revise 9E018 heading to read "Technology" from Wassenaar Munitions List; and add 9E018 sub-items for WML 22.b.1, b.2, and b.5.

6. Discrepancies in prohibited countries between ITAR and EAR

The ITAR list of prohibited countries in 126.1 is supposed to be replicated in EAR Country Group D:5. A footnote to D:5 states that, if there are any discrepancies between the two lists, the State Department list shall be controlling. On January 29, 2015, BIS added an embargo of Crimea to EAR 746.6, except for food and medicine, but did not add Crimea to D:5. DDTC has not yet added Crimea to 126.1. It makes no sense to prohibit to Crimea toothpaste and paper clips, but not items on the USML. On May 29, 2015, the State Department removed Fiji from 126.1. D:5 still includes Fiji. Remedies: add Crimea to 126.1 and to 740 Supplement 1 Country Group D:5 and delete Fiji from D:5.

7. Establish new ITAR sections of part 120 to read:

Subject to ITAR

(a) Except for items excluded in paragraph (b) of this section, the following items are subject to the ITAR:

(1) All USML-controlled "commodities," software, and "technology" (*i.e.*, all "defense articles" and "defense services") located in the United States, including in a U.S. Foreign Trade Zone or moving in-transit through the United States from one foreign country to another; and

(2) All U.S.-origin "defense articles" and "defense services" wherever located;

(b) The following are not subject to the ITAR:

(1,2,3,4) (From proposed 120.6(b)(3)(i, ii, iii, iv), re public domain, fundamental research changing 120.46 to 120.49), scientific principles, and patents, and delete 120.6 Note to paragraph (b).
(a) and (b)(1-4) would harmonize with EAR 734.3(a)(1), (a)(2), and (b)(3).)

(5) Basic marketing information on function, purpose, or general system descriptions of defense articles;

(6) Telemetry data per XV Note 3.
((b)(5) and (6) would harmonize with 120.10(b) exclusions from "technical data.")

Commodity

Commodity means any item except software or technology.
(This would harmonize with the EAR definition of "commodity.")

Technology

Technology means "technical data" or "defense services"
(This would harmonize with EAR and Wassenaar.)

8. Revise ITAR 120.6, 120.9, and 120.46 and EAR 772.1 definition of "peculiarly responsible," as follows:

120.6 **Defense article, revise to read:**
Defense article means any commodity, software, or technical data controlled on the United States Munitions List.

120.9 **Defense services:**
In (a)(1) change "directly related to" to "required for";
In Note 1 to paragraph (a)(1) change "directly related to" to "required for" (twice).
(This would harmonize with EAR and Wassenaar.)

120.46 **Required:**
In (a), change "technical data" to "technology" (three times);
In Note 2 to paragraph (a):
change "technical data" to "technology" (twice);
change "enumerated" to "controlled";
change "to which it is directly related" to "for which it is required"; and
change"directly related to" to "required for";
Revise Note 3 to paragraph (a) to read:
"Technology" "peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions" is, nevertheless, not controlled if:
(1, 2, 3, 4, 5 from proposed Note 3)

(Recommended changes in paragraph (a), in Note 2 to paragraph (a), and to remove from Note 3 that technical data for a defense article is controlled regardless of the performance level, characteristic, or function would harmonize with EAR and Wassenaar.

Changing "enumerated" to "controlled" in Note 2 would retain on the USML technical data specifically described there using catch-all language excluded from enumerated.

The recommended retention in Note 3 of decontrol parameters would harmonize with the recommended portion of the BIS proposed definition of "peculiarly responsible.")

772.1 peculiarly responsible, revise to read:
"Technology" "peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions" is, nevertheless, not controlled if:
(1, 2, 3, 4, 5, 6 from proposed definition)

9. In subcategories for technical data and defense services on the USML, change
Technical data (see 120.10 of this subchapter) and defense services (see 120.9 of this subchapter) directly related to the defense articles described in ...
to

Software "specially designed" for and "technology" "required" for "commodities" (and software) controlled by ...

10. Revise ITAR 120.11 and 120.49 and EAR 734.3, 734.7, 734.8, 734.11, Supplement 1 to part 734, and 740.9(c), as follows:

120.11 public domain:

In (a) insert following new (a)(1) and renumber (2) through (5) as (3) through (6):

(1) Sales at a price not exceeding the cost of reproduction and distribution;

Delete 120.11(b)

120.49 fundamental research

In (a)(1), delete "located"

Add the following new Note 3 to paragraph (a):

Pursuant to NSDD 189, where the national security requires control of information generated during federally-funded fundamental research in science, technology, and engineering at colleges, universities, and laboratories, the mechanism for control is classification. No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification.

Delete and Reserve 120.49(b) (on prepublication review) and delete the three Notes to paragraph (b)

(Proposed Note 2 to paragraph (a) provides adequate guidance for privately sponsored fundamental research. Recommended Note 3 to paragraph (a) provides adequate guidance for federally-funded fundamental research.)

734.3(b)(3)(i):

change "Are "published"," to "Are already published, or will be published"; and

add: "(the EAR do not cover technology that is already publicly available, as well as technology that is made public by the transaction in question)"

734.7 Published

In (a) insert following new (a)(1) and renumber (2) through (5) as (3) through (6):

(1) Sales at a price not exceeding the cost of reproduction and distribution;

734.8 fundamental research

after the semi-colon at the end of (b)(1), add "or"

at the end of (b)(2), change "; or" to a period

delete (b)(3); delete Note 2 to paragraph (b); insert following new (c), reletter (c) to (d)

(c) Pursuant to NSDD 189, where the national security requires control of information generated during federally-funded fundamental research in science, technology, and engineering at colleges, universities, and laboratories, the mechanism for control is classification. No restrictions may be placed upon the

conduct or reporting of federally-funded fundamental research that has not received national security classification.

734.11 Government-sponsored research covered by contract controls

Delete

734 Supplement 1 Questions and answers - technology and software subject to the EAR

Retain, rather than delete as proposed

Delete Question A(4) Research under DOE grant requiring prepublication DOE clearance

Delete Answer to A(6) and substitute:

No, provided that:

the government has not classified any of its content;
you did not include, or otherwise use, any classified information in its preparation;
your intent is to make it available generally to the public;
during its preparation, you agreed to no private pre-publication review; and
you have not sold it, or advertised it for sale, at a price exceeding the cost of reproduction and distribution.

Delete Answer to D(11) and substitute:

Yes, provided that:
the government has not classified any of its content;
you did not include, or otherwise use, any classified information in its preparation;
your intent is to make the research available generally to the public;
during its preparation, you agreed to no private pre-publication review; and
you have not sold it, or advertised it for sale, at a price exceeding the cost of reproduction and distribution.

Delete Answer to E(1) and substitute:

Pursuant to 120.49 Note 3 to paragraph (a) and 734.8(c) (as recommended above), the only permissible restriction on federally-funded fundamental research is classification. You should ask the DOD sponsor to withdraw the prepublication review requirement.

Delete 740.9(c) beta test software

(The expressions "intended for distribution to the general public" and "free-of-charge or at a price that does not exceed the cost of reproduction and distribution" make this "not subject to the EAR," so that no license exception is needed.)

Analysis

Imagine you are a journalist writing a story on the impact of U.S. bombers in Iraq and Syria. You read in Note 1 to paragraph (a) of 120.46, on "required," that "any technical data, regardless of significance, peculiar to making an aircraft a bomber" is controlled. Almost anything you write about a bomber could be construed as somehow related to making it. You clearly intend to put

your story in the public domain. But you note removal of sales at newsstands from the definition of public domain. Moreover, you read in 120.11(b): "Technical data or software, whether or not developed with government funding, is not in the public domain if it has been made available to the public without authorization from (a U.S. government official)." So you seek such authorization. You then discover that, for similar reasons, not only newspapers in general but also other media, advertising agencies, and academic researchers are also seeking such authorizations, often for their entire content, out of an abundance of caution. The government is overwhelmed and cannot respond within the deadlines demanded by the applicants. Moreover, the courts cannot cope with the deluge of lawsuits alleging unconstitutional prior restraint of free speech. So, reporters, advertisers, and researchers, not wishing to stop their vocations nor to significantly delay publishing, advertising, or sharing research results with the public, feel obliged to make their information publicly available without government authorization. They would thereby incur the risk of "administrative, civil, and possible criminal penalties under other law," per 734 Supplement 1 E(2). This quotation would be deleted but would probably still be applicable.

The proposed 772.1 definition of "peculiarly responsible" would ambiguously over=ride the substance of the existing Wassenaar and EAR definition of "required" and a key part of the EAR definition of "specially designed." Those terms are used in hundreds of places in the CCL. The ambiguities would cause incredible confusion in industry. Exporters would inevitably make varying interpretations. These are national security rules. Such confusion would be a significant threat to national security. That threat can easily be avoided by simply retaining the existing definitions of "required" and "specially designed" unchanged.

Ad Hoc Coalition for Effective Export Control Reform
1717 Pennsylvania Avenue, N.W. – Suite 1025
Washington, DC 20006

August 3, 2015

VIA E-MAIL (publiccomments@bis.doc.gov AND DDTCPublicComments@state.gov)

Ms. Hillary Hess
Director, Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
Washington, DC 20230

Mr. C. Edward Peartree
Director, Office of Defense Trade Controls Policy
Directorate of Defense Trade Controls
U.S. Department of State
PM/DDTC, SA-1, 12th Floor
Washington, DC 20522

REF: RIN 0694–AG32 (BIS) AND RIN 1400-AD70 (DDTC)

RE: Comments on Proposed Revisions to Certain EAR and ITAR Definitions

Dear Ms. Hess and Mr. Peartree:

The Ad Hoc Coalition for Effective Export Control Reform ("CEECR")[1] appreciates the opportunity to comment on the proposed rules published by the U.S. Department of Commerce, Bureau of Industry and Security ("BIS") and the U.S. Department of State, Directorate of Defense Controls ("DDTC") on June 3, 2015 (80 Fed. Reg. 31505 and 80 Fed. Reg. 31525, respectively) concerning proposed revisions to certain definitions in the Export Administration Regulations ("EAR") and the International Traffic in Arms Regulations ("ITAR") (individually, the "BIS Proposed Rule" and the "DDTC Proposed Rule," and collectively, the "June 3 Proposed Rules").

The CEECR believes that the expressed aims, scope, and substance of the June 3 Proposed Rules are linked to those set forth in the proposed rule on Wassenaar Arrangement 2013 Plenary Agreements Implementation that BIS published on May 20, 2015 (80 Fed. Reg. 28853) (RIN 0694-AG49) (the "May 20 Proposed Rule" or the "Wassenaar Arrangement Implementation Rule"). Accordingly, Section XI contains comments relating to the May 20 Proposed Rule for consideration by BIS.

---

[1] The Ad Hoc Coalition for Effective Export Control Reform ("CEECR") includes the following individuals: Geoffrey M. Goodale, Managing Member, Trade Law Advisors, PLLC (Washington, DC); Andrea Fekkes Dynes, Staff Vice President and Associate General Counsel, General Dynamics (Falls Church, VA); Kay C. Georgi, Partner, Arent Fox LLP (Washington, DC); Gwendolyn W. Jaramillo, Partner, Foley Hoag LLP (Boston, MA); Jonathan M. Meyer, Attorney-at- Law (New York, NY); Jason I. Poblete, Partner, Poblete Tamargo LLP (Washington, DC); Christopher B. Stagg, Partner, Stagg Noonan LLP (Washington, DC); Roland L. Trope, Partner, Trope & Schramm LLP (New York, NY); Michael L. Burton and Douglas N. Jacobson, Members, Jacobson Burton PLLC (Washington, DC) (on behalf of TRW Automotive U.S. LLC d/b/a ZF TRW and other firm clients). The comments set forth in this submission are fully supported by these individuals, but they do not necessarily reflect the views of the entities by which they are employed or whom they represent.

The CEECR applauds the U.S. Government's efforts to amend the EAR and the ITAR as part of the Obama Administration's ongoing Export Control Reform ("ECR") initiative. It is quite apparent from the text of the June 3 Proposed Rules, from comments that agency officials have made regarding on the June 3 Proposed Rules, and from the experience of our members in analyzing the June 3 Proposed Rules that much thought went into the proposed definitions that are referenced in the June 3 Proposed Rules.

In our view, many of the proposed definitions that are set forth in the June 3 Proposed Rules represent significant improvements over earlier versions of proposed definitions that have previously been issued by BIS and DDTC. However, it is the CEECR's view that the proposed definitions for certain terms under the EAR and ITAR could be further improved by making the changes or clarifications that are recommended below.

I. "Export" and "Reexport" Under the EAR and the ITAR

A. "Subject to the EAR" in Proposed EAR § 734.13 and EAR § 734.14

In the BIS Proposed Rule, the term "subject to the EAR" is not referenced in the proposed definition of "export" under EAR § 734.13, whereas that term has been used in connection with the current definition of "export" under the existing EAR. For purposes of clarity, the CEECR recommends that the term "subject to the EAR" be added in the applicable places in the proposed definition for "export" under EAR § 734.13. Specifically, we propose that the term "of items subject to the EAR" be inserted after the words "shipment or transmission" in subsection (a)(1). We also propose adding the words "subject to the EAR" before the words "to a foreign national" in subsection (a)(2), before the words "in clear text" and the words "to a foreign national" in subsection (a)(6), and before the words "to a foreign national" in subsection (b).[2]

Similarly, we recommend adding the term "subject to the EAR" and additional changes to proposed EAR § 734.13(c) so that the text would read as follows.

> The export of an item subject to the EAR that will transit through a country or countries to a destination country, or will be transshipped in a country or countries to a destination country, or are intended for export to the ~~new~~ destination country, is deemed to be an export to the ~~new~~ destination country and not to the countries of transit or transshipment.

This recommended text also has the benefit of adding clarity by substituting the term "destination country" for the term "new country" that exists in the proposed definition referenced in the BIS Proposed Rule and by adding the phrase or replacing the term "new country" in several places in sections 13(c) and 14(c) with the "and not to the countries or transit or transshipment" at the end of the proposed definition.

[2] *See* also Section I.B.1 for additional recommended changes to proposed EAR § 734.13(a)(6) and related proposed EAR § 734.14(a)(4).

For the reasons discussed above, the CEECR also recommends that conforming changes along the lines discussed above be made to the applicable parts of the proposed definition of "reexport" in proposed EAR § 734.14. Specifically, the CEECR proposes that the term "subject to the EAR" be added after the words "shipment or transmission" in subsection (a)(1), before the words "to a foreign national" in subsection (a)(2), and before the words "to a foreign national" in subsection (a)(4). We note that subsections 734.14(b) and (c) already include the phrase "subject to the EAR", as we have proposed should be the case in the corresponding subsections of proposed section 734.13.

B. Proposed New Definition for Export – Release or Transfer of Decryption Keys, Network Access Codes, Passwords, etc.

1. Proposed EAR § 734.13(a)(6)
(And Conforming Changes to Proposed EAR § 734.14(a)(4))

Under the BIS Proposed Rule, the proposed definition for "export" under EAR § 734.13(a)(6) reads as follows:

> (6) "releasing or otherwise transferring decryption keys, network access codes, passwords, 'software,' or other information with 'knowledge' that such provision will cause or permit the transfer of other 'technology' in clear text or 'software' to a foreign national." (emphasis added).

The CEECR understands that the BIS does not intend to include in the definition of export the mere act of releasing decryption keys, network access codes, passwords, 'software,' or other information but rather intends to focus on those situations where an individual undertakes such an act with knowledge that it will cause and result in a transfer of the EAR-controlled technology or software. However the word "permit" is overly broad as any release of decryption keys, network access codes, passwords, 'software,' or other information could technically "permit" such access.

The CEECR also believes that the terms "cause or permit" may be overly broad with regard to access issues and do not match the "result in" terminology in proposed EAR § 764.2(l). We believe the terms "cause or permit" could be interpreted more broadly than BIS intends, to include scenarios in which, for example: (a) a person has a decryption key stored in a briefcase in the same room as a foreign national who does not even know that the decryption key is in the briefcase because this might in theory "permit" the foreign national to have access to the decryption key; or (b) during a factory tour a foreign person receives access to an area adjacent to an area containing controlled information and breaks into the area containing controlled information. Under the latter scenario, taking the person on the factory tour may be one of the "causes" of the break-in, but it is certainly not a "sufficient cause." As such, the CEECR favors using the term **"result in**" instead of "cause or permit."

In addition, the CEECR believes that using the qualifier "in clear text or 'software'" within proposed paragraph (a)(6) could result in some confusion. This is because some exporters might not think drawings, diagrams, specifications or other non-prose information is included within the term "clear text" or "software." In the preamble to the BIS Proposed Rule, BIS has

indicated that "[t]he meaning of 'clear text' in the proposed definition is no different than an industry standard definition, e.g., information or software that is readable without any additional processing and is not encrypted. Comments are encouraged regarding whether a specific EAR definition of the term is warranted and, if so, what the definition should be." While the term "clear text" may have an industry definition within the computer/information security industry, we are uncertain that it has a uniform meaning in that industry, or that its meaning is generally known within other industries.

For the reasons discussed above, the CEECR recommends that proposed EAR § 734.13(a)(6) be revised to read, in relevant part, as follows:

> (6) "releasing or otherwise transferring decryption keys, network access codes, passwords, 'software,' or other information with 'knowledge' that such provision will result in ~~cause or permit~~ the transfer of other 'technology' in unencrypted format ~~clear text~~ or 'software' in source code format to a foreign national." [3]

Alternatively, if BIS wishes to retain the term "clear text" in proposed EAR § 734.13(a)(6), the CEECR proposes that BIS define the term "clear text" to mean "information that is readable without further decryption." In addition, the CEECR recommends that BIS provide additional clarification regarding the term "software" since BIS is proposing to exclude from the definition of "export" transfers of object code to foreign nationals. See proposed EAR § 734.13(a)(2).

Furthermore, for all of the reasons discussed above, the CEECR recommends that conforming changes along the lines of those proposed above be made to the proposed definition of "reexport" in proposed EAR § 734.14(a)(4).

2. Proposed ITAR § 120.17(a)(6)
(And Conforming Changes to Proposed ITAR §120.19)

Like the expansion of the definition of "Export" under the EAR, the new proposed ITAR § 120.17(a)(6) addresses the release or transfer of decryption keys, network access codes, passwords, software to a foreign person. However, the proposed ITAR definition differs significantly from the proposed EAR in the following two respects. First, unlike the EAR, the ITAR definition includes in the definition of "Export" the mere act of "providing physical access that would allow access to other technical data." Second, unlike the EAR, the ITAR definition includes in the definition of "Export" situations where **no** technical data has been or will be transferred to a foreign person. In the preambles to the referenced proposed rules, both DDTC and BIS have requested input from the public regarding the different formulations for this control.

[3] *See* also Section I.A. for additional recommended changes to proposed EAR § 734.13(a)(6) and related EAR § 734.14(a)(4).

The CEECR believes that the proposed revised definition for "Export" in ITAR § 120.17(a)(6) is overly broad because, as written, it captures scenarios where a foreign person has been provided mere physical access to decryption keys, network access, or passwords but no actual transfer of ITAR-controlled technical data occurs. See similar discussion above relating to EAR § 734.13(a)(6) for examples of situations where mere physical access does not result in any export of controlled information, as a matter of fact. As written, the definition would capture all situations where "access" was provided (perhaps by mistake), regardless of other facts such as period of time involved (unfettered long-term access versus short-term access) and the reality of whether technical data was actually transferred to a foreign person as a matter of fact.

For all the reasons discussed above, the CEECR recommends that proposed ITAR § 120.17(a)(6) be revised to read as follows:

> (6) Releasing or otherwise transferring ~~information such as~~ decryption keys, network access codes, passwords, software, or other information with knowledge that such provision will result in the transfer of other in unencrypted format or 'software' in source code format to a foreign person.

Furthermore, for all of the reasons discussed above, the CEECR recommends that conforming changes along the lines of those proposed above be made to the proposed definition of "reexport" in ITAR § 120.19.

II. "Release" Under the EAR and the ITAR

A. Proposed EAR § 734.15

The CEECR commends BIS for seeking to create a new definition for the term "release" under proposed EAR § 734.15. As noted in the preamble to the BIS Proposed Rule, the proposed new definition of "release" would only apply to inspections of an item or applications of knowledge or technical experience that "actually reveal controlled technology or source code" to a foreign national. See 80 Fed. Reg. 31505, 31508 (June 3, 2015). The preamble goes on to explain that "merely seeing equipment does not necessarily mean that the seer is able to glean any technology from it and, in any event, not all visible information pertaining to equipment is necessarily 'technology' subject to the EAR." We believe the language in the definition of release is reasonably clear when read together with the preamble to the proposed rule.

However, after the new definition becomes effective, it may not be completely clear when reading the definition alone what BIS intended by the term "inspection", and by the two references to conduct that "reveals" technology or source code subject to the EAR to a foreign national. To ensure the language in the EAR is clear on its face, without also having to find and review the preamble to the proposed rule, we recommend that BIS take the following actions:

(a) replace the phrase "visual or inspection" with "visual or other examination" or "close inspection by visual or other means"; and

(b) to replace the two instances of the term "reveals" with the term "actually reveals" or "actually conveys".

In addition, for the reasons discussed above under section I.A, the CEECR proposes adding the words "subject to the EAR" after the words "by a foreign national of items" in proposed EAR § 734.15(a)(1) and before the words "in the United States or abroad" in proposed EAR § 734.15(a)(2).

B. Proposed ITAR § 120.50

The CEECR agrees with the decision by DDTC to create and define the term "release" under proposed ITAR § 120.50 and for taking actions to make that definition consistent with the definition of "release" under proposed EAR § 734.15. For the reasons discussed above, the CEECR also recommends that conforming changes along the lines discussed above relating to EAR § 734.15 be made to the applicable parts of proposed ITAR § 120.50, except that the term "subject to the EAR" language should not be added anywhere in proposed ITAR § 120.50.

III. "Activities that are not exports reexports, or transfers" Under the EAR and ITAR

A. Proposed EAR § 734.18

Under proposed EAR § 734.18(a)(4), certain activities are excluded from the proposed definitions of export, reexport and transfer, including:

> (4) sending, taking, or storing technology or software that is:
>
> (i) Unclassified;
>
> (ii) Secured using end-to-end encryption;
>
> (iii) Secured using cryptographic modules (hardware or software) compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, ..., or other similarly effective means; and
>
> (iv) Not stored in a country listed in Country Group D:5 (*see* Supplement 1 to part 740 of the EAR) or in the Russian Federation. (emphasis added).

The CEECR recommends that BIS clarify its intention that an electronic transmission (*e.g.*, an e-mail) which may *transit* a country in Country Group D:5 or in the Russian Federation, and which otherwise meets the requirements of subsection (4), falls within the scope of activities that are not exports, reexports, or transfers. Specifically, such electronic transmissions are not "stored" in a country listed in Country Group D:5 or the Russian Federation. Thus, for example, a party sending an email that contains technology subject to the EAR, using end-to-end encryption and meeting the other requirements of subsection 4 can rely on such an electronic transmission *not* to constitute an export, reexport or transfer provided the party does not know that the email server is located in Country Group D:5 or in the Russian Federation.

B. Proposed ITAR § 120.52

Under proposed ITAR § 120.52, certain activities are excluded from the proposed definitions of export, reexport and transfer, including:

> (4) sending, taking, or storing technical data or software that is:
>
> (i)Unclassified;
>
> (ii) Secured using end-to-end encryption;
>
> (iii) Secured using cryptographic modules (hardware or software) compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications; and
>
> (iv) Not stored in a country proscribed in §126.1 of this subchapter or the Russian Federation. (emphasis added)

The CEECR recommends that DDTC clarify its intention that an electronic transmission (such as an email) which may *transit* a country proscribed in §126.1 of this subchapter or the Russian Federation, and which otherwise meets the requirements of subsection (4), falls within the scope of activities that are not exports, reexports, or retransfers. Specifically, such electronic transmissions are not "stored" in a country proscribed in §126.1 of this subchapter or the Russian Federation. Thus, for example, a party sending an email that contains unclassified technical data, using end-to-end encryption and meeting the other requirements of subsection 4 can rely on such an electronic transmission *not* to constitute an export, reexport or transfer provided the party does not know that the email server is located in a country proscribed in ITAR § 126.1 or in the Russian Federation.

IV. "Activities that are not 'deemed reexports'" Under the EAR

A. The Term "Is Certain" in Proposed EAR § 734.20

In the BIS Proposed Rule, proposed EAR § 734.20(a)(2) states that a "deemed reexport" does not occur if an entity:

> [i]s certain that the foreign national's most recent country of citizenship or permanent residency is that of a country to which export from the United States of the "technology" or "source code" at issue would be authorized by the EAR either under a license exception, or in situations where no license under the EAR would be required." (emphasis added)

Significantly, the term "certain" is not defined in the current EAR or in the BIS Proposed Rule, and as such, use of the term may cause confusion. Moreover, as a practical matter, it is not generally possible for companies to achieve 100% certainty about the citizenship or residency status of nationals of their own country, let alone dual or third country nationals.

The CEECR does not believe that the intent of BIS was to set an impossibly high standard or to create a strict liability standard under which a company may be found liable for improperly reexporting to a dual/third country national even if the company reasonably relies on ordinary identification documents, passports, visas, etc. to determine the nationality or residency of an individual. However, if that was BIS's intent, we do not believe that such a strict liability standard is appropriate. Non-U.S. entities that receive controlled items and technology should be allowed to use ordinary means of determining the citizenship or residency of an individual. Requiring them to achieve "certainty" could effectively stifle cooperation with close allies because it would make it far harder for companies inside close U.S. allies U.S. to collaborate with U.S. companies on export-controlled projects, which collaboration it is a major objective of export reform to promote.

For the reasons discussed above, the CEECR recommends that the term "has knowledge" be substituted for the term "is certain" in applicable places in proposed EAR § 734.20(a)(2). The CEECR believes that the term "has knowledge" is more clear (and consistent with other portions of the EAR) than the term "is certain" and is more in line with the objectives of BIS.

B. Proposed EAR §§ 734.20(b)-(c)

Proposed subsections (b) and (c) of proposed EAR § 734.20 exclude from the concept of "deemed reexport" other releases of technology or source code, by an entity outside the United States, to foreign national employees, if the employee is a national only of a country in Country Group A:5, or if certain specified clearances, screening measures or safeguards are in place. One of the requirements for the subsection (b) and (c) exclusions from the concept of "deemed reexport" is that the "release of 'technology' or 'source code' takes place entirely within the physical territory" of a country in Country Group A:5, or the country in which the entity releasing the technology or source code "is located, conducts official business, or operates."

Modern electronic communications often involve conduct falling within the definition of "release" that occurs in more than one location. It will often be the case that a release of U.S.-origin technology or software could be said to take place partially within the United States and partially within the country in which the foreign person employee is located. In each case we believe that it would be consistent with the purposes of these exceptions, and would make them more practical and straightforward to apply, if the restriction on the location of the release also included the physical territory of the United States. For these reasons, the CEECR proposes that the words "or within the physical territory of the United States" be added at the end of each of subsections (b)(4) and (c)(3) of proposed EAR § 734.20.

V. "Knowledge" and "Violations" Under the June 3 Proposed Rules

A. Proposed EAR § 764.2(l)

Under proposed EAR § 764.2(l), it is stated that the "release" or transfer of data security-related information (*e.g.*, decryption keys, network access codes, or passwords) "with 'knowledge' that the release will result, directly or indirectly, in an unauthorized export, reexport, or transfer of the 'technology'" will constitute a violation to the same extent as a violation in connection with the export of the controlled "technology" or "software." The CEECR supports the inclusion of a knowledge qualifier in this proposed new CEECR of the EAR.

However, the CEECR notes that the terms "directly or indirectly" may be confusing when speaking of decryption keys and access issues. This is because transferring or releasing an encryption key or granting access is inherently only an indirect way to export technology or software. Use of the term "indirect" here raises numerous questions, such as (a) whether failing to secure all possible vulnerabilities against hackers (an impossibility) would in and of itself constitute a violation (because there is knowledge that this could "indirectly" result something), and (b) whether failing to properly train an employee who falls victim to a "phishing" attack is a violation (because there is knowledge that a foreign national might "indirectly" use the attack to steal export controlled technology or software). Accordingly, the CEECR proposes that the terms "directly or indirectly" be deleted from proposed EAR § 764.2(l).

B. Inconsistency of Statements on "Knowledge" in the Preamble and the BIS Proposed Rule

The BIS Proposed Rule indicates that the term "knowledge" within the definition of "export" would limit the scope of the term "export." However, in the preamble to the BIS Proposed Rule, BIS raises the issue of whether a party that acts without "knowledge" may still be guilty of violations. BIS states that the proposed rule would:

> Add text prohibiting the release or other transfer of information (e.g., decryption keys, passwords or access codes) with knowledge that such release or other transfer will result in an unauthorized export, reexport or transfer of other technology or software. This addition provides specific grounds for bringing charges with respect to one particular type of misconduct. However, existing EAR provisions, including the prohibition on causing, aiding or abetting a violation of the EAR or license, authorization or order could be used to bring charges for that same type of misconduct.

80 Fed. Reg. at 31513 (emphasis added).

The CEECR is concerned that the underlined language above is in tension with the stated intent to use a knowledge qualifier within the proposed definitions of "export" and "reexport" set forth in the BIS Proposed Rule. The above language appears to say that the "same type of conduct" that is not a violation because there is no "knowledge" of a transfer could nevertheless be considered "causing, aiding or abetting a violation." Our understanding is that BIS's intention

was to say that "causing, aiding or abetting a violation of the EAR or license, authorization or order could be used to bring charges for other or related conduct even if there is no "knowledge" that a transfer will occur with respect to transfer of a particular technology or software." Accordingly, the CEECR requests that BIS provide clarification on this issue in the final rule.

C. Proposed ITAR §§ 127.1 (a)(6) and §127.1 (b)(4)

The DDTC Proposed Rule would add two new subsections describing activities that constitute violations of the ITAR.

- Proposed ITAR § 127.1(a)(6) would make it unlawful "to export, reexport, retransfer, or otherwise make available to the public technical data or software if such person has knowledge that the technical data or software was made publicly available without an authorization described in CEECR 120.11(b) of this subchapter. (emphasis added).

- In contrast, proposed ITAR § 127.1(b)(4) would make it unlawful "to release or transfer information, such as decryption keys, network access codes, or passwords that would allow access to other technical data in clear text or to software that will result, directly or indirectly, in an unauthorized export, reexport, or retransfer of the technical data in clear text or software. Violation of this provision will constitute a violation to the same extent as a violation in connection with the export of the controlled technical data or software." (emphasis added)

In proposed ITAR § 127.1(a)(6), DDTC does not penalize the act where an individual exports/reexports/retransfers information obtained from a public resource, such as the Internet, when such individual does not have knowledge that information is subject to ITAR. Rather, DDTC criminalizes the act where the individual exports, reexports, transfers such information with knowledge that it contains ITAR-controlled technical data or software which was made publicly available without an authorization.

However, proposed ITAR § 127.1(b)(4) does not similarly address those situations where an individual acts with or without knowledge; but rather it equally penalizes both acts. As a result, for example, an individual who provides (perhaps mistakenly) a network password to a foreign person without knowledge that it will result in access to technical data, would be liable for such acts – *even when no actual export of ITAR-controlled technical data result*s.

The strict liability approach taken in proposed ITAR § 127.1(b)(4) is inconsistent with proposed ITAR § 127.1(a)(6) (which would result in no liability for mistaken acts, even though an actual export of ITAR-controlled technical data would result). Proposed ITAR § 127.1(b)(4) also would be inconsistent with proposed EAR § 764.2(1), which has a knowledge requirement similar to that of ITAR § 127.1(a)(6). *See* discussion above in Section V.A.

The CEECR urges DDTC to revise proposed ITAR § 127.1(b)(4) to be consistent with proposed ITAR § 127.1(a)(6) in terms of including a knowledge or scienter requirement, which also would be consistent with proposed EAR § 764.2(1). Specifically, we recommend that proposed ITAR § 127.1(b)(4) be revised as follows to make it unlawful:

> "to release or transfer information, such as decryption keys, network access codes, or passwords **with knowledge that such provision will result**, directly or indirectly, in an unauthorized export, reexport, or retransfer of the technical data in clear text or software."

In addition, we propose that a safe harbor be created for instances in which the release or transfer of decryption keys, network access codes, or passwords does not actually result in the disclosure of technical data in clear text or software to a foreign person. We recommend that the following language be added to create such a safe harbor:

> "Violation of this provision will be **presumed to** constitute a violation to the same extent as a violation in connection with the export of the controlled technical data or software **unless the exporter can establish to the Department's satisfaction that the release or transfer of the decryption keys, network access codes or passwords, did not result in the actual access to technical data in clear text or to software by a foreign person.**"

VI. "Required" and "Peculiarly Responsible" Under the BIS Proposed Rule

A. Proposed Definitions of "Required" and "Peculiarly Responsible" Under EAR § 772.1

The BIS rule adds a definition to "required" stating that the term refers "only to that portion of 'technology' and 'software' that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions." The BIS then defines "peculiarly responsible" by using a catch and release technique employed under the "specially designed" section of the EAR and ITAR.

The CEECR believes that, due to the unique nature of technology and software, using the "catch and release" technique is a both significant departure from the EAR's General Technology Note and an expansion of the controlled technology and software that will no longer be based on the technology or software being responsible for achieving control parameters.

The current EAR contain an element of causality in its definition of "required" in the following example, which is maintained in the current proposed definition of required:

> For example, assume product "X" is controlled if it operates at or above 400 MHz and is not controlled if it operates below 400 MHz. If production technologies "A", "B", and "C" allow production at no more than 399 MHz, then technologies "A", "B", and "C" are not "required" to produce the controlled product "X". If technologies "A", "B", "C", "D", and "E" are used together, a manufacturer can produce product "X" that operates at or above 400 MHz. In this example,

technologies "D" and "E" are "required" to make the controlled product and are themselves controlled under the General Technology Note. (See the General Technology Note.)

In other words, even though technologies A, B and C are used to produce controlled product X, because they contribute nothing to making product X operate at or above 400 MHz – the control level – they are not controlled. In other words, to use plain English,

- A, B and C are not "required" – they are not "wanted, needed or called for" to use the Webster's definition[4] -- to produce that characteristic;

- A, B and C are also not "peculiarly responsible" – they are not "exclusively"[5] "answerable as the primary cause motive or agent"[6]

But if we use the new 'catch and release" definition proposed for "peculiarly responsible," all three technologies are "caught" because they are "used in or for use in the development, production or use" of the controlled item in question. And there is no guarantee that they will be "released" under (b)(3)-(b)(6). The technologies/software may only be used in or for use in the development or production the controlled item and not an EAR99 or AT-controlled item that is in "production" – not because they cause the properties that are the reason for the control – but simply because they are not used elsewhere. And as a lesser technology or software, there may not be the design history or documentation necessary to meet the other reasons for release. In short, the catch and release may result in over-control of the A, B and C types of technology and software that are not important to the reasons for control, but just happen to be for use in or for use in the development production or use of the controlled item.

The CEECR believe that the technologies that the BIS seeks to control are those that can usefully be thought of as a "but-for" cause of an item achieving a specified level or threshold of performance. In the above-example, technologies "D" and "E" would qualify as "but-for" causes of a product "X" operating at or above 400 MHz. The focus on the "but-for" causes of performance is lost in the "catch and release" definition proposed for "peculiarly responsible." Whereas the use of a "but-for" cause approach would be far easier for exporters to understand and implement, would result in a more intuitive and consistent definition of "peculiarly response", and would avoid extending the control to technologies for which there would not appear to be a need or reason for control.

It should also be noted, that, by eliminating the causal link between the

---

[4] Webster's New International Dictionary of the English Language, 2117 (1942) (to "require" is "to demand or exact as necessary or appropriate; hence, to want; to need; to call for…") (hereinafter "Webster's").

[5] Webster's at 1801 (defining "peculiar" as an "exclusive property or privileged . . .")

[6] Webster's at 2124 (defining "responsible" as "answerable as the primary, cause, motive, or agent, whether good or evil, creditable or chargeable with the result.")

technology/software and the controlled commodity, the catch and release definition is changing the definition from that found in the dictionary – and the Wassenaar Arrangement (which does not define the term "peculiarly responsible") to a very different definition found in neither the dictionary nor the Wassenaar Arrangement.

Put another way, just because a technology or software is used in or for a controlled item, and is not used in or for a non-controlled item (according to the proposed "catch and release" definition), does not mean that the technology or software is "wanted, needed or called for," to use the Webster's definition of "required," or "exclusively" "answerable as the primary cause motive or agent," to use the Webster's definition of "peculiarly responsible" for making the item controlled. In short, the proposed definition might well cause the United States to interpret the term significantly differently the other Wassenaar Members.

Finally, the CEECR respectfully submits that the catch and release principals of "specially designed" are much more easily applied to parts, components, attachments and accessories, then it is to technologies. Due to its nature, it is more difficult to determine which technologies are used in different products, making the release part of the task particularly difficult to apply in real life.

In light of these concerns, the CEECR recommends that BIS omit the "catch and release" definition of "peculiarly responsible" and allow exporters to continue to rely on the dictionary definitions of "peculiarly responsible" and the A,B,C,D and E example provided in the "required" definition.

VII. "Required" Under the DDTC Proposed Rule

A. ITAR § 120.46

The DDTC Proposed Rule adds proposed ITAR § 120.46, stating that the term "required" refers "only to that portion of technical data that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions." There are several recommendations that the CEECR wishes to make to this proposed definition of "required."

As an initial matter, the CEECR notes that proposed ITAR § 120.46 does not make reference to "software." Given that the definition of "required" under proposed EAR § 772.1 makes reference to both "technology" and "software," we believe that the omission of the term "software" in proposed ITAR § 120.46 was an inadvertent error on the part of DDTC. Accordingly, the CEECR recommends that DDTC include the term "software" in the proposed definition of "required" when final rule is issued.

Second, for the same reason set forth above, the CEECR believes that DDTC should BIS omit the "catch and release" definition of "peculiarly responsible" and allow exporters to continue to rely on the dictionary definitions of "peculiarly responsible."

If DDTC continues to use the "catch and release" definition of "peculiarly responsible," however, the CEECR has the following suggestions.

First, the CEECR believes that proposed Paragraph 5 to proposed Note 3 to paragraph (a) of proposed ITAR § 120.46 should be revised. Proposed Note 3 to paragraph (a) to proposed ITAR § 120.46 states that technical data is peculiarly responsible for achieving or exceeding controlled performance levels, characteristics or functions "if it is used in or for use in the development . . . , production . . . , operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article unless . . . 5. It was or is being developed for use in or with general purpose commodities or software (*i.e.* with no knowledge that it would be for use in or with a particular commodity)" (emphasis added).

For consistency and clarity, the CEECR recommends that DDTC revise Paragraph 5 to proposed Note 3 to paragraph (a) of proposed ITAR § 120.46 by substituting the phrase "defense article" for the phrase "particular commodity." There are several reasons why such action would be beneficial.

First, we note that DDTC's primary interest is in regulation of technical data associated with defense articles. Moreover, our understanding is that DDTC does not intend to use this note to control technical data pertaining to general use commodities, even if there is knowledge of which general use commodity it will be used with (*i.e.*, a "particular commodity").

Second, the recommended change reconciles Note 3, paragraph 5 with Note 3, paragraph 4. Paragraph 4 excepts technical data that was, or is being, developed with knowledge that it is for use in or with both defense articles and commodities not on the U.S. Munitions List. Without some revision along the lines suggested here, paragraphs 5 could be read to carve out technical data that was developed with knowledge that it would be used with both defense articles and non-defense articles, while controlling technical data developed without knowledge that it would be used with a defense article. This does not appear to be consistent with the DDTC's concern for regulating defense articles.

Third, the recommended substitution harmonizes the Note 3 with the corresponding proposed revisions to the EAR set forth in the BIS Proposed Rule relating to the proposed definition for the term "peculiarly responsible" in proposed revisions to proposed EAR § 772.1. Specifically, the BIS Proposed Rule carves out of the definition of "Peculiarly responsible" various scenarios, including when an item "was or is being developed with 'knowledge' that it would be for use in or with commodities or software described in … an ECCN controlled for AT-only reasons and also EAR99 commodities or software…." (proposed EAR § 772.1, "Peculiary responsible, subparagraph (6).) Commodities or software falling under ECCNs controlled for reasons only of AT or under EAR99 are under less restrictive export controls than other items that are "peculiarly responsible" for achieving controlled performance levels. Our proposed recommendation relating to ITAR § 120.46, Note 3, paragraph 5 would render the proposed term "required" consistent with the proposed EAR definition of "peculiarly responsible" in this respect.

B. ITAR § 120.41

We note that the proposed definition of "required" tracks with the ITAR's existing definition of "specially designed" (*see* ITAR § 120.41), and that the existing definition of "specially designed" contains similarly unclear language in paragraph (b)(5), referring to "a

particular commodity (*e.g.*, a F/A-18) or type of commodity (*e.g.*, an aircraft or machine tool)" when "a particular defense article (e.g., a F/A-18 or HMMWV) or type of defense article (e.g., an aircraft or machine tool)." It does not appear that there was any discussion of this aspect of the definition of "specially designed" in the promulgation of CEECR 120.41. *See* 78 Fed. Reg. 22747 (Apr. 16, 2013). As such, we recommend that DDTC also revise the definition of "specially designed" to substitute the words "particular defense article" for "particular commodity" and "type of defense article" for "type of commodity in ITAR § 120.41(b)(5).

VIII. Proposed ITAR § 120.9 – "Defense Service"

Under DDTC's Proposed Rule, proposed ITAR § 120.9(a)(2) and its corresponding note provide:

> (2) The furnishing of assistance (including training) to a foreign person (see § 120.16), whether in the United States or abroad, in the development of a defense article, or the integration of a defense article with any other item regardless of whether that item is subject to the ITAR or technical data is used;
>
> Note to paragraph (a)(2): ''Integration'' means any engineering analysis (see § 125.4(c)(5) of this subchapter) needed to unite a defense article and one or more items. Integration includes the introduction of software to enable operation of a defense article, and the determination during the design process of where an item will be installed (e.g., integration of a civil engine into a destroyer that requires changes or modifications to the destroyer in order for the civil engine to operate properly; not plug and play). Integration is distinct from ''installation.'' Installation means the act of putting an item in its predetermined place without the use of technical data or any modifications to the defense article involved, other than to accommodate the fit of the item with the defense article (e.g., installing a dashboard radio into a military vehicle where no modifications (other than to accommodate the fit of the item) are made to the vehicle, and there is no use of technical data.). The ''fit'' of an item is defined by its ability to physically interface or connect with or become an integral part of another item.

80 Fed. Reg. at 31534 (emphasis added to highlight text of particular concern).

Having reviewed the text of proposed ITAR § 120.9(a)(2) and the note thereto, as well as DDTC's responses to prior comments, we believe that DDTC's conditioning the term "installation" on there being "*no* use of technical data" is overbroad and could have significant negative consequences across a number of industries. As discussed below, we believe the proposed text of the Note has a number of drawbacks.

Inconsistency Between Section 120.9(a)(2) and its Note. To begin with, there is inconsistency between proposed ITAR § 120.9(a)(2) and its Note. The proposed text of Section 120.9(a)(2) defines "defense service" "*regardless of whether . . . technical data is used*." The corresponding note, however, then makes the use of *any* technical data dispositive with regard to whether the service will be treated as "integration" rather than merely "installation" – apparently even when limited to "fit." Thus, the proposed rule and note read in conjunction are internally

inconsistent because, as proposed, the determination of whether a defense service is rendered is not without regard to the use of technical data.

Receipt / Use of Technical Data is Common and Often Necessary When Specially Designing Components for Defense Articles. In addition, proposed ITAR § 120.9(a)(2) and its Note fail to recognize that the receipt and use of technical data is common and often necessary when specially designing components for defense articles. In the automotive, aerospace, and maritime sectors, for example, it is common for defense contractors manufacturing military platforms or their subsystems to contract with commercial suppliers for specific parts and components. As is commonly known, the form factor of these parts and components often must be modified in a variety of ways to fit the vehicle or aircraft, or an assembly thereof. Indeed, the transfer of jurisdiction from DDTC to BIS over such "600 Series" items expressly acknowledges this issue and has been a major goal and achievement of the ECRI.

As part of the process of developing, modifying, and manufacturing commercial items specially designed for use in defense articles, it is common and often necessary (though not always the case) that the manufacturer of the platform will provide certain technical data regarding the vehicle so the commercial component supplier can make appropriate modifications to the component to ensure that the form factor of the component will allow it to "fit" the vehicle – i.e., to physically interface or connect with or become an integral part of another item.

Which technical data is shared with the component manufacturer is determined by the vehicle manufacturer. In some cases, the vehicle manufacturer will provide very limited technical data regarding only those vehicle systems into which the component must fit. In other cases, the vehicle manufacturer might provide a broader range of data about the vehicle. In relatively few cases, however, would a defense contractor provide no technical data to component manufacturers that are specially designing components for a defense article.

Our concern, therefore, is that registration as a manufacturer / exporter under the ITAR and obtaining a Technical Assistance Agreement or other authorization under the ITAR would be required in many (or even most cases) merely to modify a commercial item for installation into a defense article – in addition to obtaining BIS authorization for export of the item.

Proposed Rule Threatens to Undercut ECR By Requiring DDTC *and* BIS Licenses for 600 Series Items. Moreover, as written, proposed ITAR § 120.9(a)(2) and its Note threaten to undercut the ECRI by in effect requiring both DDTC *and* BIS licenses for 600 Series Items. This potential dual licensing (and registration) requirement is inconsistent with and threatens to undercut what is a hallmark of the President's ECRI. With due respect to differing perspectives, if the intent were to transfer control over specially designed components of defense articles to BIS but continue to regulate under the ITAR the process of component design and manufacture, the very rationale of the reform is called into question from the standpoint of industry. In short, we would urge great care in not allowing an (unintentionally) overbroad explanation of "integration" to gut the significant and welcome efficiencies that the ECRI has promised and can achieve. We note further that any such dual licensing is likely to be identified by foreign customers who will seek foreign sources of supply to "engineer around the ITAR."

Modification / Engineering Analysis of the Defense Article *Beyond* Component "Fit" Is a More Reasonable Basis for Control under section 120.9(a)(2), Not Whether Technical Data was Provided or Relied Upon When Specially Designing the Component. Modification/engineering analysis of the defense article *beyond* component "fit" is a more reasonable basis for control under proposed ITAR § 120.9(a)(2), not whether technical data was provided or relied upon when specially designing the component. Whether a defense service is deemed to be exported would be more reasonably and objectively determined by the nature of the engineering analysis or "integration" provided to the foreign recipient (*i.e.*, the service), not the technical data provided to or relied upon by the component manufacturer specially designing a commercial item for "installation" into the defense article. We understand DDTC's interest in asserting control over major modifications to the military platform *beyond* "fit." For the reasons set forth above, however, we do not believe that modifications limited to "fit" – regardless of whether technical data is used – should be controlled as a defense service.

Introduction of Software Must Be "Required" for the Operation of a Defense Article to Constitute A Defense Service. On a separate but related issue, the CEECR has concerns regarding DDTC's proposal to include in the definition of "integration" for purposes of the Note the following text: *"Integration includes the introduction of software to enable operation of a defense article…."* The language as proposed is significantly overbroad and should be revised.

Numerous examples come to mind where introducing or installing software on a defense article should not be controlled as a defense service – e.g., installing a commercial operating system (such as Windows 10) on a Category XI defense article. The CEECR believes it would be more appropriate to base the control of software introduction on whether the software introduced and/or some unique feature of the installation itself is "required" for operation of the defense article.

We recommend that the introduction of the software must be "required" – i.e., "peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions." Using such a defined term also is preferable to the undefined term "enable" in that it furthers the goal of consistency of interpretation across sections of the ITAR and the EAR.

As discussed above under Part VII, the CEECR believes that DDTC and BIS should omit the "catch and release" definition of "peculiarly responsible" and allow exporters to continue to rely on the dictionary definitions of "peculiarly responsible." Moreover, we urge DDTC to revise the proposed definition of "required" in the ways discussed above under Part VII.

DDTC Should Harmonize Proposed ITAR §§ 120.9(a)(1) & (a)(2) to Preserve Distinction Between Installation and Integration. In its response to comments on the prior proposed rules regarding ITAR §120.9, DDTC writes:

> The modifications of the ''defense article'' to accommodate the fit of the item to be integrated, which are within the activity covered by installation, are only those modifications to the ''defense article'' that allow the item to be placed in its predetermined location. Any modifications to the design of a ''defense article'' are beyond the scope of installation. Additionally, while minor modifications may be made to a ''defense article'' without the activity being controlled under (a)(2)

> as an integration activity, *all modifications of defense articles, regardless of sophistication, are activities controlled under (a)(1) if performed by someone with prior knowledge of U.S.-origin ''technical data.''*

80 Fed. Reg. at 31531 (emphasis added to highlight text of particular concern).

If DDTC intends to accept any of CEECR's comments and suggested revisions to ITAR §120.9(a)(2), then some harmonization is required to resolve the apparent trumping of subsection (a)(2) by (a)(1), if the person performing the installation has prior knowledge of U.S.-origin technical data. We believe this could be accomplished with additional clarifying language in the Note to subsection (a)(2) and have suggested this below.

In addition to our concerns about the impact on subsection (a)(2), the CEECR believes that DDTC's defining whether a defense service is rendered by virtue of whether an engineer has knowledge of technical data is again overbroad. While we appreciate DDTC's attempts to limit in certain respects what type of technical data an engineer might have in her head that would rise to the level of performing a defense service (e.g., technical data related to the same USML category as the current project), we believe it remains overbroad and not as well defined as industry would hope.

Under the current proposed rule, an engineer who had prior knowledge of technical data in Category XI could not perform any modification related to another Category XI item (even mere installation) without having rendered a defense service. We need not remind you how broad certain categories of the USML remain even after ECRI. We believe a more logical approach would be break the defense service analysis into elements to look at several factors to determine whether a defense service had been rendered, including for example, (1) knowledge and (2) use of (3) U.S.-origin (4) technical data (5) "required" (6) to modify (among other types of activities) (7) a defense article (8) beyond "installation" / "fit."

We do not mean to suggest that this is a perfect alternate formulation, but it illustrates that the issue contains more facets than an engineer's knowledge of technical data, which would benefit from a more refined rule. We note that the proposed revision to the Note to proposed subsection (a)(2) below does not alleviate this broader concern with (a)(1). It should, however, reconcile the tension between the two provisions.

Proposed Revision. For the reasons discussed above, the CEECR recommends that DDTC revise the Note to paragraph (a)(2) of proposed ITAR § 120.9 as follows (deletions are indicated with strike-throughs and additions are in small caps):

> **Note to paragraph (a)(2):** ''Integration'' means any engineering analysis (see § 125.4(c)(5) of this subchapter) needed to unite a defense article and one or more items. Integration includes the introduction of software ~~to enable~~ "required" for operation of a defense article, and the determination during the design process of where an item will be installed (e.g., integration of a civil engine into a destroyer that requires changes or modifications to the destroyer in order for the civil engine to operate properly; not plug and play). Integration is distinct from ''installation.'' Installation means the act of putting an item in its predetermined place without ~~the~~

~~use of technical data or~~ any modifications to the defense article involved, other than to accommodate the fit of the item with the defense article (e.g., installing a dashboard radio into a military vehicle where no modifications (other than to accommodate the fit of the item) are made to the vehicle~~, and there is no use of technical data~~.). The ''fit'' of an item is defined by its ability to physically interface or connect with or become an integral part of another item. ([S]ee § 120.41). *A TRANSFER OF TECHNICAL DATA OR OTHERWISE HAVING KNOWLEDGE OF TECHNICAL DATA RELATED TO "FIT" OR PROVIDED FOR THE PURPOSE OF ACCOMMODATING THE "FIT" OF AN ITEM IN A DEFENSE ARTICLE IS NOT ITSELF SUFFICIENT TO ESTABLISH "INTEGRATION" (E.G., LIGHT ARMORED VEHICLE MANUFACTURER PROVIDES A STEERING COLUMN MANUFACTURER TECHNICAL DATA REGARDING THE VEHICLE OR ITS SUBSYSTEMS TO ENABLE MODIFICATIONS TO A COMMERCIAL STEERING COLUMN, BUT NO TECHNICAL DATA RELATED TO MODIFICATIONS TO THE VEHICLE (OTHER THAN TO ACCOMMODATE THE FIT OF THE STEERING COLUMN) ARE TRANSFERRED FROM THE STEERING COLUMN MANUFACTURER TO THE VEHICLE MANUFACTURER).*

We believe that the suggested revisions above, including the addition of the last sentence, would be a reasonable solution to accommodate industry's concerns – yet still safeguard national security interests.

Manufacturing and Production Consulting Services. U.S. persons that are consultants in specialized manufacturing and production optimization processes and techniques, such as Six Sigma and Lean Manufacturing, are often asked by foreign manufacturers of defense articles to provide consulting services in this area. The current definition of "defense services" is so broad that such services are captured when the services are associated with the manufacture or production of foreign defense articles.

While the proposed changes to ITAR § 120.9(a)(1) removes the term "manufacture" from the current definition and adds language attempting to limit the scope of "assistance" considered to be a defense services, the proposed definition may still unintentionally capture Six Sigma or Lean Manufacturing techniques associated with the production of a foreign defense article. For example, it is possible that a U.S person who may have obtained some "knowledge of U.S. origin technical data directly related to the defense article that is subject to the assistance, prior to the performing of the service" in the foreign country. However, the mere knowledge of ITAR controlled technical data should not be sufficient to capture a production-related consulting service if the information conveyed is general in nature and does not change the technical specifications or military characteristics of a foreign defense article. For example, a U.S. person consultant may provide guidance to a foreign defense article manufacturer on how to optimize workflows of a production line used to manufacture defense articles. Similarly, a U.S. person consultant may recommend the use of a particular commercial-off-the-shelf adhesive in lieu of the current one being used. In both cases, the services provided should not be considered a defense service.

As a result, we recommend that an additional note to paragraph (a) be included as an example of an activity that is not a defense service:

> 10. The furnishing of consulting services to a foreign person in the production of a foreign defense article, such as Six Sigma or Lean Manufacturing techniques, as long as the information conveyed does not rely on U.S. origin technical data and does not change the technical specifications or military characteristics of a foreign defense article.

Absence of Comments on Other Aspects of Proposed ITAR § 120.9 Should *Not* Be Viewed as CEECR's Endorsement of Those Subsections. These comments primarily address certain elements of proposed ITAR § 120.9(a)(2) and its Note. We urge DDTC, however, not to infer from the lack of comments on other aspects of the rule that the CEECR endorses the rest of the proposed rule. While this version of proposed ITAR § 120.9 represents a significant improvement over prior proposed rules on defense services, the CEECR believes additional thought should be dedicated to this section in particular, given the complexities associated with controlling defense services. We would be happy to present additional comments to DDTC regarding other concerns and opportunities for improvement of the proposed rule.

IX. "Public Domain" Under the DDTC Proposed Rule

A. Public Domain-Related Assertions Relevant to Proposed ITAR § 120.11

In the preamble to the DDTC Proposed Rule, DDTC asserts that a requirement to obtain prior approval from DDTC or certain other U.S. Government agencies or officials before technical data can be deemed to be in the public domain, even if it has already been released to the public, is not a new requirement and is actually a currently existing requirement. The CEECR disagrees with this assertion and urges DDTC to revisit the history of this issue, and reconsider the proposed definition of Public Domain.

As an initial matter, it is important to note that a previously written prior approval requirement under the ITAR was repealed in 1984 due to First Amendment concerns. These concerns were expressed to DDTC by the Department of Justice on three occasions in 1978, 1981 and 1984. In addition, in 1981, the U.S. Congress recommended to the State Department that the ITAR be revised to avoid First Amendment issues.

Additionally, in a review of court cases involving the Arms Export Control Act since that time, DDTC has not asserted a prior approval requirement to put information into the public domain. In one case from 1996 that is directly tied to this discussion, an exporter in 1994 filed two commodity jurisdiction (CJ) requests. *See Karn v. Dep't. of State*, 925 F. Supp. 1 (D.D.C. 1996). In the first request, the exporter requested a determination of a textbook that concerned cryptography. The textbook included source code in print and on a diskette in an electronic text file. The second CJ request held that the source code on the diskette was ITAR-controlled software even though it was the identical source code that was printed in the textbook.

Of importance here, even though the textbook in *Karn* admittedly contained information required for the design, development, assembly, and manufacture of a defense article (*i.e.*,

technical data), DDTC held that the textbook was in the public domain. However, the textbook was published prior to the CJ determination. There is no evidence that indicates prior approval from the author or publisher of this textbook to place it into the public domain was sought or granted by DDTC. Similar to all the "technical data" published in other textbooks, journals, conferences, open meetings and on the Internet, it is doubtful that prior approval to publish the textbook was sought or required by DDTC. If it believed that prior approval was required to publish the book, DDTC did not articulate that view or, apparently, take steps to enforce it.

Since that court case, we are unaware of any other publicly known claim from DDTC that there is a prior approval requirement to put information into the public domain. Even in the ongoing litigation in *Defense Distributed v. Dep't. of State*,[7] DDTC has taken the position that "the regulations . . . carve out a wide exemption for 'public domain' data that helps ensure [the ITAR's] reach is appropriately limited. . . . For this reason, there is simply no substantial overbreadth here." Government Brief in Opposition at 22 (June 10, 2015).

While we note, that as a legal matter, the definition of public domain relates to an exclusion from the scope of the ITAR rather than an exemption from an otherwise subject ITAR requirement, even DDTC admits in federal court that without a public domain exclusion there would be constitutional issues under the First Amendment. If DDTC's position is that there is a prior approval requirement to use an exclusion, then there is no public domain exclusion at all.

In addition, the CEECR notes with concern that DDTC's assertion of a prior approval requirement to use the public domain exclusion provided in the definition of "technical data" in ITAR § 120.10(b) means that fundamental research performed by the academic and scientific community at accredited institutions of higher learning in the United States requires prior approval from the U.S. Government. It is difficult to imagine a scenario where DDTC's asserted prior approval requirement on academic and scientific speech by the university community would survive First Amendment scrutiny.

For all of the reasons discussed above, the CEECR urges DDTC revisit the history of this issue, and reconsider the proposed definition of Public Domain and confirm there is no existing prior approval requirement.

B. Proposed ITAR § 120.11(b)

It is the CEECR's view that proposed ITAR § 120.11(b), which relates to the prior approval requirement to put information into the public domain discussed above, would amount to an unconstitutional prior restraint. Moreover, even if the provisions set forth in proposed

---

[7] While we have knowledge of this court case and DDTC's May 8, 2013 letter to Defense Distributed that implies a prior approval requirement, we note that this is legally insufficient to serve as legally recognized public notice. DDTC's private letter to Defense Distributed was not made public by DDTC but by Defense Distributed. Further, we only have knowledge of the lawsuit that was filed in 2015, because it was brought by Defense Distributed. DDTC has taken no action itself to make its material interpretation of the law known to the public.

ITAR § 120.11(b) were content-neutral, the First Amendment still requires that the U.S. Government establish specific procedural safeguards, and as written, the prior approval requirement lacks such constitutionally required procedural safeguards. Accordingly, the CEECR urges DDTC not to include proposed ITAR § 120.11(b) when issuing the final rule.

The procedural safeguards required under the First Amendment to impose a lawful prior restraint are: "(1) any restraint prior to judicial review can be imposed only for a specified brief period during which the status quo must be maintained; (2) expeditious judicial review of that decision must be available; and (3) the censor must bear the burden of going to court to suppress the speech and must bear the burden of proof once in court." *FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 227-228 (1990).

Here, the ITAR expressly exempts judicial review of approval and licensing decisions in ITAR § 128.1, and it concedes that it is a "highly discretionary" system. Further, there are no strict timelines for a licensing or approval determination to be made. Additionally, there is added delay in receiving an approval because of the required Congressional notification under Section 38(f) of the Arms Export Control Act. The AECA also expressly prohibits judicial review of designations of items as on the U.S. Munitions List.

Significantly, a federal court already has held that key aspects of the ITAR were an unconstitutional prior restraint that failed to provide any procedural safeguards. *See Bernstein v. Dep't. of State,* 945 F. Supp 1279, 1289 (N.D. Cal. 1996). In that case, the court stated that "[t]he ITAR scheme, a paradigm of standardless discretion, fails on every count, and further noted that "[t]his. court finds nothing in the ITAR that places even minimal discretion of the licensor and hence nothing to alleviate the danger of arbitrary or discriminatory licensing decisions." Id. at 1286. The federal court even drew attention to DDTC ignoring a discussion on procedural safeguards in defending the lawsuit. Id. at 1286 ("[DDTC's] arguments . . . are notable for the conspicuous absence of discussion of the prior restraint doctrine ").

In light of the above precedent, and considering that proposed ITAR § 120.11(b) does not provide the constitutionally required safeguards, the CEECR urges DDTC not to include proposed ITAR § 120.11(b) when issuing the final rule.

C. Proposed ITAR § 120.11 – Note 1

Note 1 to proposed ITAR § 120.11 makes no distinction between public domain and restricted information, and as such, it can be read to require government authorization before publishing, disseminating, or exporting any and all information. This is an undue burden that would require submission to the U.S. Government of every journal article, speech, book, and manuscript prior to any attempts to publish them. It would put undue liability on anyone who receives such potential information as requiring proof that consent from the government was obtained in order to publish said information, and there is no format or methodology given for obtaining this consent. For all of these reasons, the CEECR recommends that DDTC not include Note 1 to proposed ITAR § 120.11 when issuing the final rule.

D. Proposed ITAR § 120.6(b)(3)(iii)

Proposed ITAR § 120.6(b)(3)(iii) states that items that "concern general scientific, mathematical, or engineering principles commonly taught in schools . . ." are not defense articles subject to the ITAR. The CEECR requests that the word "general" be deleted as it is not defined and could limit what is covered to only entry-level courses as opposed to a broad range of scientific instruction.

Significantly, courts have held that only information "significantly and directly related to defense articles" are subject to the ITAR. *See United States v. Edler Industries*, 579 F. 2d 516 (9th Cir. 1978). It is hard to imagine that any scientific, mathematical, or engineering principles *commonly* taught in schools is "significantly and directly related to" a defense article. Thus, by only excluding "general" information that is *commonly* taught in this academic context rather than any information *commonly* taught in this academic context, proposed ITAR § 120.6(b)(iii) fails to follow the holding of *Edler*.

DDTC is already on the public record that it maintains such a narrow construction:

> In recent years, some parts of the academic community have expressed concern about the application of government export regulations to disclosures of information in university classrooms. This concern (for example, that the language of the ITAR was overly broad) did not occur because of any changes in the text of the ITAR, or in the policies and practices of the Department of State in administering the regulations. In order to address the concerns expressed about the regulations, however, the language with regard to what information is subject to ITAR controls has been clarified. The Department's long-standing practice of regulating only information that is directly related to defense articles, as reflected in U*.S. v. Edler*, 579 F. 2d 516 (9th Cir. 1978), remains unchanged. *See* 49 Fed. Reg. 47,683 (Dec. 6, 1984).

For all of the reasons discussed above, the CEECR urges DDTC to delete the word "general" from proposed ITAR § 120.6(b)(iii) in accordance with DDTC's long-standing adherence to only controlling technical data that is significant and directly related to a defense article.

In addition, the CEECR notes that the lack of a definition of the term "directly related" under the ITAR is problematic. As a matter of law, the AECA only provides the legal authority to control defense services (as defined by ITAR § 120.9), software (as defined by ITAR § 120.45), and technical data (as defined by ITAR § 120.10) that are directly related to a defense article. Therefore, defense services, software, or technical data that are not "directly related" to a defense article are not controlled on the USML, and items not controlled on the USML are not subject to the statutory authorities under the AECA. As such, the "directly related" requirement is a material qualifier. The ABA further notes that the only control criteria on software is for software directly related to a defense article, which in the absence of a definition will result in different understandings within government and industry.

Although DDTC is now proposing a definition of "required" under proposed ITAR § 120.46, the CEECR notes that the AECA is limited to only controlling defense services, software and technical data that are "significant and directly related to defense articles" as required by the narrowing construction in *United States v. Edler*. While DDTC is satisfying the first limitation with a definition of "required," it is not defining the second limitation of what "directly related" means. Further, as proposed, there would be no means to know what constitutes software "directly related" to a defense article.

For all of these reasons, the CEECR recommends that the meaning of "directly related" be defined by DDTC to ensure common understanding within industry and the government as to what constitutes a defense service, technical data, or software that is "directly related" to a defense article.

E. Proposed ITAR § 120.47 and Proposed ITAR § 120.49

The proposed definition of "development" in proposed ITAR § 120.47 and its distinction from "fundamental research" under proposed ITAR §120.49(c) needlessly restricts research. "Fundamental research" often involves activities included in the proposed definition of "development" such as design research, design analysis, and testing of prototypes to conclude whether a hypothesis being testing is correct. For example, it is often necessary to build some sort of prototype to determine if calculations in engineering and mathematics match a real-world application. Such activities should not be considered "development" since they are simply forms of testing that many research institutions perform. In view of this fact, the CEECR urges that such activities should be stricken from the definition of "development" in proposed ITAR § 120.47.

The definition of "fundamental research" under proposed ITAR § 120.49(c) includes the phrase "this is distinguished from . . . industrial development." The term "industrial" is not defined, but if it is taken as the definition of "development" in proposed ITAR § 120.47, such interpretation could lead to unintended consequences, such as potentially hampering the advancement of science and technology being made at universities. Also, such interpretation would conflict with proposed ITAR § 120.49(c)(2)(ii)(*Applied Research* definition), which includes the effort that, in part, "attempts to determine and exploit potential scientific discoveries . . .," because an amount of development is often required to ensure that sound theories and good ideas can be put into practice. As such, the CEECR urges that DDTC strike the word "development" from proposed ITAR § 120.49(c) and expand the definition of "applied research" under proposed ITAR § 120.49(c)(2) to include development within the context of fundamental research that is intended for publication.

X. "Fundamental Research" Under the BIS Proposed Rule

A. Proposed EAR § 734.3(b)(3)(iii)

Proposed EAR § 734.3(b)(3)(iii) states that information and software that "concern general scientific, mathematical, or engineering principles commonly taught in schools . . ." are not subject to the EAR. For the same reasons discussed above under CEECR VII.D, the CEECR

urges that the word "general" be deleted from proposed EAR § 734.3(b)(iii) since that word is not defined and could limit what is covered to only entry-level courses as opposed to a broad range of scientific instruction.

B. Proposed EAR § 734.8(b) – Note 2

Proposed revised EAR § 734.8 concerns technology that arises during, or results from, fundamental research, and excludes certain such technology from the scope of the EAR if certain conditions are met (e.g., intended to be published). As written, Proposed Note 2 to paragraph (b) could cause a requirement to renegotiate many government contracts held with universities and any companies that engage in fundamental research in an attempt to remove the clause lest the status of research as fundamental be challenged, creating unnecessary and undue burdens on researchers.

In contrast, proposed Note 2 to proposed ITAR § 120.49(b)is preferable to Proposed Note 2 to proposed EAR § 734.8(b). Proposed Note 2 to proposed ITAR § 120.49(b) states: "Research that is voluntarily subject to U.S. government prepublication review is considered intended to be published for all releases consistent with any resulting controls." This is interpreted to mean that prepublication review does not necessarily impede a fundamental research designation.

For all of the reasons discussed above, and to promote consistency between the ITAR and the EAR, the CEECR recommends that the same or similar language to that contained in proposed Note 2 to proposed ITAR § 120.49(b) be used in Proposed Note 2 to proposed EAR § 734.8(b).

C. Proposed EAR § 734.8(c)

Proposed EAR § 734.8 does not explicitly state that software resulting from fundamental research is "not subject to the EAR." This is in stark contrast to the way in which software is treated under current EAR § 734.8. The CEECR proposes that language should be added to Proposed EAR § 734.8 that explicitly states that software resulting from fundamental research is "not subject to EAR."

Another key concept from existing EAR § 734.8 also is omitted from proposed EAR § 734.8. Specifically, current EAR § 734.8(b)(1) contains the phrase "research conducted by scientists, engineers, or students at a university normally will be considered fundamental research," but proposed EAR § 734.8(c) is missing this phrase. The CEECR recommends that this language from current EAR § 734.8(b)(1) be included in proposed EAR § 734.8(c). We believe that this wording should be carried to the proposed rules to make clear what is covered.

XI. Issues Relating to the BIS May 20, 2015 Wassenaar Arrangement Implementation Rule Proposed Rule

A. Timing of Final Rule Implementation

If the effective date for the final rule relating to the Wassenaar Arrangement Implementation Rule is scheduled to be on or shortly after the final rule's publication date, the CEECR believes that there are serious risks that such an abrupt start to the rule will disrupt existing contracts for "cybersecurity items" and will put the parties thereto in immediate non-compliance with the rule. As explained below, the CEECR recommends that BIS establish the effective date of the final rule to be *at least six months* later than the final rule's publication date.

As proposed, the Wassenaar Arrangement Implementation Rule will apply to an unknown and potentially large number of items "not previously designated for export control." In the preamble to the May 20 Proposed Rule, BIS acknowledges that the new *cybersecurity controls* will apply export controls, and impose license requirements, on items not previously controlled by the EAR or items that previously were eligible for License Exception ENC. As BIS explains:

> "Although these cybersecurity capabilities[8] **were not previously designated for export control**, many of these items have been controlled for their 'information security' functionality, including encryption and cryptanalysis."[9]

However, neither the preamble nor the proposed rule itself addresses how BIS will bring the final rule into effect (*i.e.,* whether the publication date of the final rule will be the same as its effective date).

---

[8] The "cybersecurity capabilities" refers to preceding sentences where BIS identifies the following as "cybersecurity items":

- "**systems, equipment or components** specially designed for the generation, operation or delivery of, or communication with, intrusion software";
- "**software** specially designed or modified for the development or production of such systems, equipment, or components";
- "**software** specially designed for the generation, operation or delivery of, or communication with, intrusion software";
- "**technology** required for the development of intrusion software";
- "**Internet Protocol (IP) network communications surveillance systems** or **equipment and test, inspection, production equipment**, specially designed **components** therefor"; and
- "**development and production software and technology** therefor".

See 80 Fed. Reg. at 28853 (emphases added).

[9] *See id.*

On May 20, 2015, when BIS issued the Wassenaar Arrangement Implementation Rule, many U.S. firms may have been under contract (and perhaps multiple contracts) to export, reexport or transfer "cybersecurity items" that had not previously been designated for export control. Similarly, universities conducting "fundamental research" and development of technologies for commercialization will probably have had ongoing faculty/student research teams engaged in activities that, under the final rule, may constitute the export, reexport or transfer of "cybersecurity capabilities" not previously designated for export control.

Furthermore, between the proposal date and the final rule's publication date, additional U.S. persons will probably have entered into such contracts or will soon do so, especially in light of the fact that there has not been extensive media reportage about the proposed rule. Numerous U.S. persons that transact in "cybersecurity items" are probably still unaware of the proposed rule, and even those aware of it may not have been briefed by counsel on the compliance obligations that will arise when the rule is adopted and comes into effect.

If the final rule becomes effective immediately, many "U.S. persons", as defined in Section 772.1 of the EAR, will be at risk of failing to comply with the final rule when it comes into effect. We think such noncompliance will be the result for several reasons.

First, U.S. persons will have pre-existing contractual obligations to export, reexport or transfer "cybersecurity items" that will be newly designated for export control and subject to license requirements. Many such persons may have little, if any, awareness of the proposed rule and be unaware of the risks that the final rule may pose to their existing and contemplated contracts for "cybersecurity items" or to their internal research and development programs involving "cybersecurity items."

With respect to contracts for "cybersecurity items" that will not, by their own terms, terminate before the final rule's effective date ("Subject Contracts"), certain U.S. parties to these Subject Contracts will find themselves in a double-bind on the effective date: immediate compliance with the rule will require them to take actions that may, when taken, put them in material breach of the relevant Subject Contracts.

Parties to Subject Contracts (and their officers and directors) who are unaware of the proposed rule or unaware of the compliance obligations that the final rule will impose on their enterprises and dealings will have had no reason or opportunity to negotiate and structure such contracts in order to avert the double-bind of duties to comply with the final rule and obligations to complete performance of their Subject Contracts.

Few, if any, of the existing Subject Contracts are likely to contain provisions that condition the parties' export, reexport or transfer obligations on compliance with the final rule. Moreover, the scope and terms of the final rule may differ substantively in crucial details from the proposed rule. As a result, until the final rule is published by BIS, the officers and directors of such enterprises engaged in Subject Contracts will have no reliable knowledge of the final rule's scope and terms. Without knowledge of the precise scope and terms of the final rule, it is not practicable for parties to Subject Contracts to negotiate provisions to address that rule. For

the same reasons, counsel cannot competently advise clients on ways to address the yet-to-be disclosed version of the final rule in a Subject Contract.

Boilerplate provisions in commercial contracts might mitigate some of the transactional risks, but will probably not adequately address them or control them within the limits of a corporate client's tolerance of risks. A typical boilerplate provision that obligates all parties to a contract to "comply with all applicable U.S. export control laws and regulations", if included in a Subject Contract, would probably not avert the risks posed by the final rule coming into effect on or very soon after its date of publication by BIS. Similarly, a typical *force majeure* or event of excusable delay clause will not sufficiently reduce such risks, particularly in states (such as New York) whose courts tend to construe *force majeure* clauses narrowly.

Second, the final rule will impose broad licensing obligations on the export, reexport or transfer of "cybersecurity items" that were previously designated as EAR 99 or eligible for License Exception ENC. As a result, and because there are no license exceptions for intracompany transfers, end users or end uses, or deemed exports,[10] many U.S. companies and research organizations will be required to obtain licenses to be in compliance with the final rule as of its effective date. However, prior to the publication of the final rule, it will not be possible for U.S. persons affected by the rule to identify with certainty all the instances in which a license will be required.

Moreover, once the final rule is published, U.S. persons who engage in exports of "cybersecurity items" will need to spend considerable time and resources to identify situations in which licenses are required as well as prepare, submit and receive such licenses. In order to obtain the necessary licenses, there must be ample time between the publication of the final rule and its effective date to allow U.S. persons to assess the need for, apply for and receive the licenses required under the final rule. For companies that engage in exports of, or that design and develop "cybersecurity items" (and whose engineering staff may include foreign nationals), there may be a need to apply for and obtain multiple licenses. Without sufficient time to do so after the final rule is published, such companies will be unable to comply with applicable license requirements without bringing certain aspects of their business organization to a halt. This, of course, could disrupt contractual relationships and impose financial hardship, especially on small businesses.

As discussed above, the less time there is between the publication of the final rule and its effective date, the greater will be the risk that U.S. persons affected by the final rule will be abruptly and detrimentally confronted by their duties to comply with the final rule and their commitments to complete existing contractual obligations or ongoing research programs.

The CEECR respectfully recommends that BIS establish the effective date of the final rule to be *at least six months* later than the final rule's publication date.

[10] *See* BIS's FAQs on Intrusion and Surveillance Items posted by BIS at http://www.bis.doc.gov/index.php/policy-guidance/faqs.

A minimum of a six-month interval between publication and effective date is necessary in order for there to be sufficient time to come into compliance with the final rule. During this interval, we expect the following activities to occur:

1. U.S. persons impacted by the rule will be briefed by counsel on the scope, terms, and significance of the final rule;

2. Counsel and compliance officers will advise clients on compliance duties under the final rule, the risks of non-compliance, and the appropriate changes to export compliance programs, including training, an activity that will require significant time due to the proposed rule's complexity;

3. U.S. persons impacted by the rule will review existing and contemplated Subject Contracts to identify which existing contractual obligations may conflict with compliance obligations under the final rule and take appropriate actions, such as negotiating and executing amendments to existing Subject Contracts to avert the risk of non-compliance with the final rule while, at the same time, fulfilling contractual obligations; and

4. U.S. persons impacted by the rule will survey their business or research operations to identify the need for licenses and, if needed, will prepare, submit and wait to receive such licenses.

The CEECR believes that a six-month delay, at a minimum, between the publication date of the final rule and its effective date is necessary for U.S. persons affected by the rule to comply with their obligations under the final rule without undue hardship and the risk of substantial disruption to their business and research operations.

B. Obligations Prior to the Effective Date

The CEECR believes that companies and their counsel will be concerned about the obligations that U.S. persons may have for "cybersecurity items" that they exported, reexported, or transferred prior to the effective date of the final rule.

In particular, they will need to know the legal status of "cybersecurity items" not previously designated for export control that foreign nationals received or gained access to before adoption of the final rule. Similarly, they will need to know whether pre-rule "deemed exports" of such "cybersecurity items" trigger any obligations by the exporter to recapture or recover such items from the foreign national recipients.

The CEECR recommends that BIS consider issuing guidance (perhaps in the form of additional FAQs) that would address the status of pre-rule exported "cybersecurity items" and the compliance duties of exporters and recipients of such items – where such items have not previously been designated for export control.

C. Exporter's Knowledge

In the preamble to the May 20 Proposed Rule, it states that the "EAR also prohibits the export of equipment if the exporter intends it will be combined with other equipment to comprise a system described in the new entry." 80 Fed. Reg. at 28854 (emphasis added). While this statement suggests that only the exporter's intent matters, elsewhere in the proposed rule, it indicates that violations also can result from what the exporter knows that the recipient intends to do with the item. For example, in the proposed text for revisions to ECCN 5A001 (at 80 Fed. Reg. 28661), the language reads:

> "[S]uch equipment may not be sold separately **with knowledge** that it will be combined with other equipment to comprise a system described in the new paragraph." (Emphasis added.)

This language makes clear that the exporter's "knowledge" is the key factor.

It is the CEECR's belief that emphasis on an exporter's knowledge" is consistent with an exporter's duty to determine if the export recipient or end-user intends to make prohibited or unlicensed use of the controlled item and should be emphasized by BIS. Accordingly, assuming that this view of the CEECR is accurate, the CEECR recommends that BIS clarify (in the preamble to any final rule that is issued) that an exporter's knowledge is critical to determining whether a violation may or may not have occurred if an export recipient or end-user combines an item with other equipment to comprise a new controlled system.

D. Proposed EAR § 742.6(b)(5)

Proposed EAR 742.6(b)(5) defines "foreign commercial partner" to mean:

> a foreign-based non-governmental end-user that has a **business need** to **share** the proprietary information of the U.S. company and is **contractually bound** to the U.S. company (*e.g.,* has an established pattern of continuing or recurring contractual relations).

80 Fed. Reg. 28858 (emphasis added). As discussed below, the CEECR is concerned that each of the three underlined terms in the above definition could encourage export practices that are not intended by BIS and that would be contrary to the objectives of the EAR.

The term "**business need**" is not defined in the May 20 Proposed Rule or elsewhere in the EAR. Every activity of a business can be characterized as a "business need" when its owners or operators perceive an apparent benefit to doing so. In fact, there is little that a company cannot characterize as a "business need" if doing so will benefit the company. As a result, the term "business need" may be interpreted by exporters and export recipients so expansively as to render it applicable to almost any activity of a business. Such interpretations could easily reduce to a meaningless and thus irrelevant term an otherwise important requirement for an export recipient to qualify as a "foreign business partner." Exporters would be encouraged to accept any claim of a "business need" by the prospective end-user.

There appears to be an error in using the verb "**to share**" as the operative term in the requirement that an end-user have "a business need to "**share**" the proprietary information of the U.S. company." As used in that context, "**share**" conveys the sense that the end-user must have a business need to disclose the exporter's proprietary information *to third parties*. That meaning, of course, misdirects the criteria from what we think BIS intended, namely that the end-user represent (and the exporter verify) that the end-user has a genuine business need that will be served if the exporter will be permitted (by an export license) to *disclose the U.S. company's proprietary data* to the end-user. Unless corrected, such error will confuse exporters and may cause BIS to reject applications for licenses that fail to meet the criteria that BIS intends to establish.

The criteria for an end-user to qualify as a "foreign business partner" include the additional prong or requirement that the end-user "be **contractually bound** to the U.S. company." However, there is nothing in the words – or in the context of the definition – that delimits what kind of contractual relationship will qualify as necessary and sufficient to meet the requirement.

There is also no suggestion that the relevant contract(s) must relate to the proposed export of "cybersecurity items" that is the subject of the exporter's license application. Experienced counsel can reasonably infer that BIS intends there to be a relationship between the required exporter/end-user contract and the proposed export of "cybersecurity items". However, in a definition of this importance the objectives of the proposed rule would be far better served if exporters were not left to guess at the meaning of the requirement that the end-user be "contractually bound to the U.S. company" nor that their legal counsel be constrained to infer such meaning without reliable guidance from the text of the rule, other provisions in the EAR, or interpretations issued by BIS in the published rule or the relevant FAQs.

BIS appears to have foreseen the need for clarification of the phrase "contractually bound to the U.S. company" as evidenced by BIS's insertion of an elucidating example in the parenthetical phrase that ends the definition:

"(*e.g.,* has an **established pattern of continuing or recurring** contractual relations)."

However, in the vernacular of commercial or corporate transactions (and in the legal jargon applied to them), parties seldom, if ever, refer in contracts, agreements, or correspondence to an intention to "establish a pattern of continuing or recurring contractual relations". Thus, there is no familiar use of that phrase or a context in which it can be set that would make it susceptible of a reliable interpretation.[11] Moreover, whatever is meant by a "pattern . . . of

[11] Moreover, the term "pattern" when it serves as an operable term in laws tends to appear in litigation contexts (*e.g.,* "fact pattern") and in criminal law contexts (*e.g.,* in the definition of a RICO claim where a plaintiff or prosecutor must, among things, prove a "*pattern* of racketeering"). [Continued on next page]

contractual relations" fails to illuminate the criteria that must be met to qualify the parties as "contractually bound."

Moreover, we think that the parenthetical introduces an unintended ambiguity: the example of "contractually bound" that it gives refers to multiple contracts ("**recurring contractual relations**") and, in the alternative, to seemingly multi-year contracts that precede the submittal of the license application and that will extend for some indefinite period, possibly beyond the proposed export transaction ("**continuing contractual relations**"). In either event, the requirement ends with the word "relations" in the plural.

As a result, it is unclear whether BIS intends the example to be a limiting illustration – thereby requiring evidence that the exporter and end-user are "bound" or engaged in multiple contracts (whether "recurring" or "continuing") -- or whether BIS intends instead that the parenthetical not be a limiting example and that even one contract between the exporter and end-user will suffice. The ambiguity has an additional layer: it is unclear whether "contractually bound" requires that the proposed export be the subject of or covered by such contract(s). The members of the CEECR could not reach consensus on how to interpret the parenthetical example, which seems to suggest that the example is indeed ambiguous and that it is open to quite divergent, and possibly irreconcilable, interpretations.

In order to address the potential problems discussed above, the CEECR recommends that BIS revise the term "foreign business partner" by using the following language for the note to EAR § 742.6(b)(5):

> *"Note to paragraph (b)(5): A 'foreign business counter-party'*[12] *means a foreign based non-governmental end-user that has entered into, or proposes in writing to enter into, one or more contracts with a U.S. company and who takes appropriate actions to safeguard "cybersecurity items" to prevent the unauthorized or unlicensed reexport or transfer of such information (and include in such safeguards sufficient cybersecurity measures to prevent intrusions and exfiltration by insiders and outsiders)."*

[Continued from Footnote 11 on page 31] Such usages are unhelpful aids to interpreting the meaning of the proposed rule's phrase "an established pattern of continuing or recurring contractual relations".

[12] We note that the term "partner" denotes a legal relationship that most commercial and corporate transactions do not create and that use of the term "partner" (which can denote "partnership" or denote "counterparty") will not improve the export control of "cybersecurity items." For this reason, we recommend that BIS replace the term "partner" with "counter-party", which would suggest a contractual relationship and allow for the definition to delimit its meaning.

E. Licensing Policy for "Cybersecurity Items"

Under the proposed licensing policy set forth under the May 20 Proposed Rule, an application for export license would be "reviewed favorably" when the relevant export is destined for a U.S. company's subsidiary located in a Country Group A:5 country such as South Korea.

The CEECR is concerned by the distinction that the proposed licensing policy attempts to draw between U.S. company subsidiaries located in a Country Group A:5 country and companies located in the same country but owned instead by nationals of that Country Group A:5 country. The distinction appears to treat license applications differently where there may not be, in fact, a significant or sufficient difference to warrant not viewing favorably the application for export to a company located in and owned by nationals of the Country Group A:5 country.

We are also concerned by the distinction that the proposed licensing policy attempts to draw between "foreign commercial partners" located in a Country Group A:5 country and a company located in and owned by nationals of the same Country Group A:5 country.

If BIS does not modify the "foreign commercial partner" category, then the policy would draw a distinction that would not necessarily serve the aims of the proposed rule. The policy would discriminate in favor of, for example, South Korean companies that manage to enter into multiple contracts with a U.S. exporter and to discriminate against South Korean companies that are seeking for the first time to be end-user recipients or seeking to enter into a commercial contract or corporate transaction for the first time with a particular U.S. exporter. Note the commercially disadvantageous consequences of a licensing policy that draws such distinction:

- A highly reliable South Korean company (with a demonstrable record of respecting and complying with U.S. export controls in multiple contracts with several different U.S. companies) is the identified end-user in a license application submitted by an exporter who has not previously transacted with the South Korean company. Such an application would not qualify to be "reviewed favorably", even though the proposed end-user might be far more reliable an end-user (as measured by its export compliance policies, practices, and record) than a South Korean company that happens to have restricted its multiple transactions to one U.S. exporter (and thus might qualify as a "foreign commercial partner").

- A prospective joint venture or merger or acquisition between a U.S. company and a South Korean company would involve proposed exports or transfers of "cybersecurity items" from the U.S. company to the South Korean party to the venture or corporate transaction. The parties may not have previously engaged in commercial transactions involving licensed exports. However, the South Korean company may have all of the qualifications mentioned in the preceding bullet point.

We think in both of the above-described examples the proposed licensing policy would create unnecessary obstacles to cross-border commercial and corporate transactions that the U.S. government presumably wants to encourage. Such costly hindrances could be averted by a tightly focused revision to the licensing policy.

In order to address such potential problems, the CEECR respectfully recommends that BIS adopt the following revision to the proposed licensing policy for "cybersecurity items:"

- To the categories of license applications that would be "reviewed favorably", add a new category that would cover proposed exports of "cybersecurity items" to qualified trustworthy end-users located in Country Group A:5 countries (or a subset of such countries with whose companies it is U.S. policy to encourage transactions).

- The recommended new category would be defined as set forth in the bold text in the following excerpt of BIS' proposed description of its licensing policy:

  "Applications for exports, reexports and transfers for cybersecurity items … controlled for RS will be reviewed favorably if destined to … 'foreign commercial partners' located in Country Group A:5, ***demonstrably qualified end-users located in Country Group A:5****, . . ."*

- Add a note, immediately after the proposed *Note to paragraph (b)(5)*, which would state:

  "Additional Note to paragraph (b)(5): A 'demonstrably qualified end-user' means a nongovernmental end-user, based in a Country Group A:5 country, that meets the following criteria: the end-user must either (i) have a record of compliance with U.S. export control laws and regulations or (ii) have provided the applicant with evidence that it has adopted and implemented cybersecurity and export compliance plans reasonably designed to avert unauthorized or unlicensed reexports or transfers (in country).".

- The note should, of course, include a comparable requirement contained at the end of the existing note to paragraph (b)(5), namely the requirement for an explanatory letter that explains:

  "how the end-user meets the criteria of a 'demonstrably qualified end-user' located in a Country Group A:5 state and how the end-user will safeguard the items from unauthorized transfers (in-country) and reexports."

This recommendation to add a category for license applications for exports destined to "qualified end-users in a Country Group A:5 country" would, of perforce, provide that such applications are subject to the same precautions that the proposed policy applies to applications for exports destined to "foreign business partners": a case-by-case review to determine if the transaction "is contrary to the national security or foreign policy interests of the United States"; a "focused case-by-case review for reasons of Encryption Items (EI) control" if any "information security" functionality is incorporated in the cybersecurity item that is the subject of the license application; and, a presumptive denial if such items "have or support rootkit or zero-day exploit capabilities."

F. Proposed EAR § 748.8(z)(1)(iii)(C)

Proposed EAR § 748.8(z)(1)(iii)(C) sets forth a requirement for an applicant's explanatory letter when the "cybersecurity items" for which an export license is applied have "not been previously classified or included in a license application . . ."[13] In that context, it is clearly important to the export control of intrusion technologies that BIS be informed by the applicant when the items proposed for export incorporate the highly sensitive technologies of "rootkit or zero-day exploit functionality." However, when the items for which an export license is applied merely "relate" to "intrusion software" (which itself is *not controlled* by the proposed rule[14]), the license applicant should not be required to "**describe** how rootkit or zero-day exploit functionality is **precluded** from the item."

The problem with the proposed requirement rests in its asking applicants to generate descriptions of "zero-day exploit functionalities" that will often be impracticable to substantiate or will compel applicants to make exhaustive efforts to discover. Furthermore, for a license applicant to describe how rootkit or zero-day exploit functionality is *precluded* from its items or services will often prove to be beyond the applicant's ability to ascertain.

The term "**preclude**" suggests that applicants must make a potential outcome impossible or prevent it from happening. That is a task that engineers often pursue when designing safety features into a technology or system. We think, however, that in the context of "zero-day exploit functionality" in a technology or system that may contain millions of lines of software code the proposed requirement asks a company and its engineers to perform a task that will in all likelihood be extravagantly expensive to complete and thus economically beyond their reach. It will probably also be beyond their ability to ensure that their software code will not produce certain outcomes or features. It is well known that in designing software, the control of desired outcomes is usually achievable, whereas the control or avoidance of undesired outcomes is usually impossible to achieve.

We note that "zero day" vulnerabilities is a term that the proposed rule and the EAR do not define. We take the term to refer to vulnerabilities that are unknown to the designer or producer of a particular item. What makes "zero-day" vulnerabilities so sensitive is that the designer or producer of the item remains unaware of their existence, despite its best efforts to review and test the item for "zero-day" vulnerabilities.

As a result, if a potential attacker discovers such vulnerabilities, it can conduct exploits (often stealthily) against a defenseless target. Moreover, it is generally considered economically unjustifiable for a designer or producer of an item to discover all "zero-day" vulnerabilities in the item because that would entail every line of code be tested alone and in all combinations with other lines of code contained in the item. In fact, the prodigious size and complexity of contemporary software *precludes* discovery of every latent "zero-day" vulnerability in the code.

---

[13] *Id.*

[14] *See* BIS FAQs, No. 7, which states, in pertinent part: "Exploits that meet the definition of 'intrusion software' are not controlled."

"Zero-day" vulnerabilities have thus become the unknown feature in "cybersecurity items" that engineers know exists, but lamentably cannot ferret out.

Since many "zero-day" vulnerabilities are inherently undiscoverable by the designer or producer of an item, we think it impracticable and unwise to require a license applicant to "**describe** how rootkit or zero-day exploit functionality is **precluded** from the item." It makes little sense to attempt to describe the preclusion or avoidance of vulnerabilities that the applicant has not discovered, may be financially incapable of discovering, and thus cannot develop ways of precluding.

In short, unless modified, the requirement will put applicants to the task of describing how their item precludes the very "zero-day" vulnerabilities they do not know of. We recognize that designers and producers increasingly assume that creating products without such vulnerabilities is beyond the current capabilities of virtually all designers and producers. However, knowing that as yet undiscovered "zero-day" vulnerabilities are an inherent feature of an item does not give the designer or producer the knowledge needed to "describe" how any associated "zero-day exploit functionality is precluded from the item."

If the intent of the proposed requirement is more limited and seeks only to require that applicants describe how the design of their item prevents it from being used to exploit a "zero-day" vulnerability, the requirement as phrased does not make clear that limited scope. Moreover, even if so limited, much the same objection applies to the requirement: even items that do not contain "zero-day" vulnerabilities can be combined with other items to produce an intrusion technology and the designers of such items may not have been aware of such potential uses. Thus to require a designer or producer to describe potential uses it does not know of and to explain how it avoids them would appear to ask them to perform a futile and burdensome task.

In order to address the deficiencies discussed above, the CEECR recommends that BIS:

- Delete the requirement that an applicant "**describe** how rootkit or zero-day exploit functionality is **precluded** from the item"; and

- Replace it with the following requirement:

  "(C) For items related to 'intrusion software' provide a certification, signed by an officer of the applicant, authorized to certify on behalf of the applicant, that after a diligent inquiry, as evidenced by end-user certifications, the applicant does not know of any rootkit or zero-day exploit functionality contained in the item and does not know of any intention by the proposed end-user to combine the item with any other items to create a rootkit or zero-day exploit functionality."

By thus providing for an appropriately focused certification, the requirement would only necessitate that an applicant to perform a feasible and practicable set of inquiries.

XII. Conclusion

Your consideration of our comments is greatly appreciated. If you have any questions regarding this submission, please contact Geoffrey Goodale by telephone at (703) 618-6640 or by e-mail at ggoodale@tradelawadvisors.com.

Respectfully submitted,

Geoffrey M. Goodale

The Ad Hoc Coalition for Effective Export Control Reform

AAU *Association of American Universities*
APLU *Association of Public and Land-grant Universities*
COGR *Council on Governmental Relations*

August 3, 2015

Rose Gottemoeller
Under Secretary for Arms Control and International Security
Office of Defense Trade Controls Policy
Department of State
2401 E. Street, N.W.
Washington, D.C. 20037

Via Email: DDTCPublicComments@state.gov

Re: ITAR Amendment—Revisions to Definitions; Data Transmission and Storage (RIN 1400—AD70)

Dear Under Secretary Gottemoeller:

Enclosed please find comments from the Association of American Universities, the Association of Public and Land-grant Universities, and the Council on Governmental Relations on the ITAR Amendment – Revisions to Definitions; Data Transmission and Storage (RIN 1400-AD70). Our staff is available to provide more information or discuss these matters further should you have any questions regarding our comments.

Sincerely,

Hunter R. Rawlings III
President
AAU

Peter McPherson
President
APLU

Anthony DeCrappeo
President
COGR

Attachment 1

AAU *Association of American Universities*
APLU *Association of Public and Land-grant Universities*
COGR *Council on Governmental Relations*

MEMORANDUM

August 3, 2015

TO: **Office of Defense Trade Controls Policy, U.S. Department of State**

FROM: **Association of American Universities**
Contact: Tobin Smith, toby.smith@aau.edu (202) 408-7500
Association of Public and Land-grant Universities
Contact: Jennifer Poulakidas, jpoulakidas@aplu.org (202) 478-5344
Council on Governmental Relations
Contact: Robert Hardy, rhardy@cogr.edu (202) 289-6655

Re: **(RIN 1400—AD70)**
ITAR Amendment—Revisions to Definitions; Data Transmission and Storage

On behalf of the over 200 universities represented by our associations, we greatly appreciate the opportunity to comment on the revisions to ITAR definitions and concerning data transmission and storage (RIN 1400—AD70).

The Association of American Universities (AAU) is an association of 60 U.S. and two Canadian leading research universities organized to develop and implement effective national and institutional policies supporting research and scholarship, graduate and undergraduate education, and public service in research universities. The Association of Public and Land-grant Universities (APLU) is a research, policy, and advocacy organization of 238 public research universities, land-grant institutions, state university systems, and affiliated organizations, dedicated to increasing degree completion and academic success, advancing scientific research, and expanding engagement. The Council on Governmental Relations (COGR) is an association of 190 U.S. research universities and their affiliated academic medical centers and research institutes that concerns itself with the impact of federal regulations, policies, and practices on the performance of research and other sponsored activities conducted at its member institutions.

The proposed ITAR rule contains a number of helpful changes and clarifications (e.g. definition of "release," clarification that submission of manuscripts to journal editors constitutes "published" information). In addition, we appreciate the Department's repeated attempts to clarify the definition and scope of "defense services." This has been a longstanding issue of concern to our members. Unfortunately, there is one particular aspect of the proposed changes which we believe will largely over shadow these other positive changes.

The proposed ITAR rule would consider any proprietary information review requirement imposed by a sponsor to exclude this research from being considered fundamental, even when ultimately no information is deemed to be proprietary. This is extremely problematic and threatens to stifle university-industry research collaborations. *We therefore strongly urge DDTC to eliminate the language excluding information subject to proprietary review from being considered fundamental research and to align its language more closely with the EAR treatment of data where a sponsor requires prior review before publication.*

Prepublication Review

We appreciate that the proposed ITAR rule recognizes that information arising during, or resulting from fundamental research that is intended to be published is not technical data subject to the ITAR (and now provides a separate definition apart from "public domain" for fundamental research information). Currently the ITAR does not directly address this point.

However, the proposed rule (120.49(b) provides that "intended to be published" does not apply to research sponsor proprietary information review. In order to be considered fundamental research a researcher must be free to publish the information without any restriction or delay. This is a marked contrast from the EAR, which continues to provide that such review does not change the status of technology that arises during or results from fundamental research as still "intended to be published."

Under the proposed ITAR rule, all research agreements that involve defense articles subject to the ITAR in which publication is subject to a proprietary information review by the sponsor would not be considered fundamental research. Control plans and licenses for any foreign nationals involved in such activities would be required before projects could be undertaken.

No explanation is provided as to the reason for these different policies. The ITAR provision contradicts the intent of the reform initiative to harmonize the EAR and ITAR. More importantly, it will have a chilling effect on university-industry collaborations directly working against the Administration's efforts to increase these types of collaborations to more quickly move new ideas from the lab to the marketplace. Almost all agreements with industry sponsors include provisions for proprietary and patentable information review. Companies understandably want the ability to guard against inadvertent disclosure of their proprietary information or trade secrets in publications of research findings and results by university researchers. Without this ability industry is unlikely to enter into sponsorship of university research. However, there still is a clear intent to publish the research results. The purpose of these short-term (typically 30—60 days) delays for review is to ensure that any proprietary input data received from an industry partner is not included inadvertently in an academic publication. Such clauses do not imply in any way that the research results themselves would somehow be proprietary to the company. In fact, often universities routinely include a clause that reinforces the fact that they are academic institutions that have the right to publish research results. This situation differs significantly from situations where the sponsor must approve publication of the research results. Many universities will not accept such terms from sponsors, in large part because they are not considered fundamental research.

Universities and their faculty are being pushed by government at all levels, including the Federal government, to increasingly collaborate and work more closely with industry in an effort to quickly move products from the lab to the marketplace. Our member institutions are very aware of the need to meet these challenges while preserving the open nature of university research. The proposed ITAR provision is counter to these goals and threatens the ability of universities to achieve these objectives, particularly in defense-related areas where universities often serve as subcontractors to defense contractors for research related to particular defense technologies. It is unclear how treatment of such activities as controlled serves our national security interests. Additionally it clearly does not serve our economic interests. We have worked extensively with the Department of Defense to ensure that neither government nor sponsor approval is required for publication of fundamental research findings in such situations. Requiring licenses and control plans for research projects which are merely subject to sponsor review for proprietary information - but for which in most cases no proprietary information is in fact included - will greatly increase compliance burdens, and adversely affect the interest and ability of universities to undertake such research projects.

The proposed rule also raises serious questions of consistency with government policy on the transfer of scientific and technical information as reflected in National Security Decision Directive 189 (NSDD 189). That directive provides that "No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. statutes." It also provides that "…to the maximum extent possible, the products of fundamental research (should) remain unrestricted." The proposed

rule restricts research where the results are merely reviewable by sponsors for the possible erroneous inclusion of proprietary information. This appears an arbitrary agency decision lacking clear statutory authorization in contravention of stated government policy. We strongly urge that "…or research sponsor proprietary information review" be deleted from the proposed 120.49(b).

Fundamental Research

There is an inconsistency between the proposed §120.49 entitled "Technical data that arises during, or results from, fundamental research," and 120.6 (a)(3) which indicates that information and software that arise during, or result from, fundamental research, are not subject to the ITAR. The proposed definition of "technical data" in 120.10(a) includes information but not software. This appears to be a significant narrowing of "fundamental research." Omission of software from "fundamental research" would significantly complicate and restrict university research. While natural-language documents written by a researcher would be "technical data" that could be freely shared as arising during fundamental research, a computer-language document written by the same researcher, working on the same project (a program in source code) would be subject to deemed export restrictions. Information and software are treated the same way in the proposed definition of "public domain" (120.11) and deemed export (§120.17(a)(2)). We believe that 120.49 should be revised to apply clearly both to technical data and software.

In addition, Note 1 to paragraph 120.49(a) states that "The inputs used to conduct fundamental research, such as information, equipment, or software, are not "technical data that arises during or results from fundamental research" except to the extent that such inputs are technical data that arose during or resulted from earlier fundamental research." We believe the statement may be misleading. Conduct of fundamental research draws upon a wide range of information and other inputs. NSDD 189 does not make a distinction between the conduct and results of fundamental research, In drawing such a sharp distinction, DDTC appears to be arbitrarily restricting NSDD 189 without clear authority. We question the need for this statement, and urge that it be removed.

Defense Services

We appreciate the attempt to provide a narrower definition of "defense service," and concur with DDTC that the revised definition is unlikely to encompass normal duties of university employees. However, in the course of considering the public comments on the several previous definitions proposed for "defense services," DDTC appears to have gone somewhat to the opposite extreme in the proposed 120.9(a)(1) and now has decoupled the actual use of technical data in providing the defense service. Instead it is based on knowledge gained through participation in the development of defense articles. We believe such a subjective test will be difficult to apply in practice both for the regulated community and DDTC. There needs to be a clear connection to using the technical data in providing the assistance.

We also appreciate the distinction between "integration" and "installation" in 120.9(a))(2), which appears consistent with our previous comments on this issue. However, it appears that use of public domain information in "integration" still may be a defense service. We believe performing a defense service should be tied to use of technical data, regardless of whether it involves integration or furnishing of other assistance. We are concerned that with the new proposed definition of "integration," (a)(2) could encompass normal sharing of academic information.

We suggest DDTC consider harmonizing the education exclusion now in the proposed 120.9(a) Note 9, with the proposed revised EAR 734.3(b)(3)(iii), which merges current ITAR (120.10(b)) and EAR text. We further suggest that the language "or by instruction in a catalog course or associated teaching laboratory of an academic institution" be added to avoid unintentionally limiting this exclusion. University courses in emerging technology areas should be covered so long as they are included in course catalogues. It also would be helpful to add a note that university capstone project courses are not considered defense services.

Public Domain

The proposed ITAR 120.11 revises the definition of "public domain" to identify characteristics without limiting the definition to specific circumstances as in the current ITAR. While we agree with the intent to streamline the definition, the examples given still are primarily in terms of tangible information and do not at all recognize newer forms of information technology such as photonics. The same comment applies to other ITAR provisions, e.g. 120.17.

The provision in the proposed 120.11(b) that technical data or software is not in the public domain if it has been made available to the public without authorization from the government raises serious concerns for us. It may lead to confusion over how this provision applies to information made available to the public through any of the means listed in 120.11(a). It is not clear how data or software that already has been publicly shared through one or more of these means cannot be considered as in the public domain. No time limit is indicated in 120.11(b). Moreover the scope is not limited to government funding, and could apply to a very wide range of unclassified information from many different sources. This provision raises serious legal and policy issues. We urge DDTC to withdraw it or substantially limit its scope. Corresponding changes should be made to the proposed 127.1(a)(6). As stated this provision raises questions as to who in the chain of making technical data or software publicly available would be held responsible and what type and degree of knowledge is required for violations.

Cloud Computing

We appreciate that both the proposed EAR and ITAR rules address cloud computing situations, which have been a cause for considerable uncertainty under the current rules. In the companion rule BIS asks for comments as to which proposed rule more clearly describes the intended control. We prefer the proposed EAR definition in 734.13(a)(6), which requires knowledge that releasing information relating to encryption will cause or permit the transfer of technology to a foreign national. In general, we believe that knowledge or intent to transfer controlled information should be required for an "export" or "deemed export" to occur. We also prefer the EAR provision in 734.18(4)(iii) providing for “other similarly effective cryptographic means “ for securing technology or software to the proposed ITAR 120.52(a)(4)(iii). While the NIST standards are widely accepted, they are not necessarily followed by all our member institutions since some institutions use other means to assure effective cryptographic management.

In addition, the restriction in 120.52 (a)(iv) to countries not proscribed in 126.1 unfortunately may substantially limit the usefulness of the proposed rule. In the experience of our members, most cloud providers insist on storing data anywhere that they want. We suggest DDTC consider adding a note that a contract that imposes these obligations on a vendor is sufficient for compliance purposes, to provide a greater safe harbor. Ensuring actual compliance is beyond our members' control.

Other Comments

DDTC asks for comments on the technical aspects of data transmission and storage in 120.17. Our associations are unable to comment on these aspects, but we have encouraged our members to do so.

Note 3 to the new definition of "Required" in 120.46(a) provides a definition for "peculiarly responsible" identical to the proposed stand-alone EAR definition in 772.1. DDTC asks for comments on placement of this definition. The EAR placement seems easier to identify, but we have suggested that our members provide their own review and comments on this issue.

We also suggest that DDTC add a note to the proposed 120.47 definition of “development” to clarify that prototypes fabricated by universities solely for academic demonstration purposes with no intent to develop them for commercial production are not “development.”

Effective Date

DDTC proposes a 30-day delayed effective date. Changes to USML categories generally have had a six-month delayed effective date while other rules affecting export controls have been effective on the date of publication. Obviously the content of the final rule is an important consideration. Our view is that significant changes in definitions should have as long a lead time as possible for implementation. Therefore we support a six-month delayed effective date.

Conclusion

In closing, we believe there are many positive changes in the proposed rule. Unfortunately they are overshadowed by the proposed 120.49(b) prepublication review restriction discussed above. We strongly urge DDTC to reconsider this restriction, which is inconsistent both with stated government policy on fundamental research and on current government policy objectives as well as the goals of the export controls reform initiative to harmonize definitions.

We appreciate the opportunity to comment and are available to provide more information or discuss these matters further should you have any questions regarding our comments.